Parecer do Comité (artigo 64.º)

Parecer 28/2024 sobre certos aspetos da proteção de dados relacionados com o tratamento de dados pessoais no contexto dos modelos de IA

Adotado em 17 de dezembro de 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Síntese

As tecnologias de IA criam muitas oportunidades e benefícios numa vasta gama de setores e atividades sociais.

Ao proteger o direito fundamental à proteção de dados, o RGPD apoia estas oportunidades e promove outros direitos fundamentais da UE, incluindo o direito à liberdade de pensamento, de expressão e de informação, o direito à educação ou a liberdade de empresa. Desta forma, o RGPD é um quadro jurídico que incentiva a inovação responsável.

Neste contexto, tendo em conta as questões de proteção de dados suscitadas por estas tecnologias, a autoridade de controlo irlandesa solicitou ao CEPD que emitisse um parecer sobre questões de aplicação geral nos termos do artigo 64.º, n.º 2, do RGPD. O pedido diz respeito ao tratamento de dados pessoais no contexto das fases de desenvolvimento e implantação de modelos de inteligência artificial («**IA**»). Mais pormenorizadamente, o pedido solicitava: (1) quando e de que forma um modelo de IA pode ser considerado «anónimo»; (2) como os responsáveis pelo tratamento podem demonstrar a adequação do interesse legítimo como base jurídica nas fases de desenvolvimento e (3) implantação; e (4) quais são as consequências do tratamento ilícito de dados pessoais na fase de desenvolvimento de um modelo de IA no subsequente tratamento ou operação do modelo de IA.

No que diz respeito à primeira questão, o parecer menciona que os pedidos de anonimato de um modelo de IA devem ser avaliados caso a caso pelas AC competentes, uma vez que o CEPD considera que os modelos de IA formados com dados pessoais não podem, em todos os casos, ser considerados anónimos. Para que um modelo de IA seja considerado anónimo, tanto 1) a probabilidade de extração direta (incluindo probabilística) de dados pessoais relativamente a pessoas cujos dados pessoais foram utilizados para desenvolver o modelo como 2) a probabilidade de obter, intencionalmente ou não, esses dados pessoais através de consultas, deve ser insignificante, tendo em conta «*todos os meios razoavelmente suscetíveis de serem utilizados*» pelo responsável pelo tratamento ou por outra pessoa.

Para realizarem a sua avaliação, as AC devem analisar a documentação fornecida pelo responsável pelo tratamento, a fim de demonstrar o anonimato do modelo. A este respeito, o parecer fornece uma lista não prescritiva e não exaustiva de métodos que podem ser utilizados pelos responsáveis pelo tratamento de dados na sua demonstração de anonimato e, por conseguinte, ser considerados pelas AC ao avaliarem a alegação de anonimato de um responsável pelo tratamento de dados. Tal abrange, por exemplo, as abordagens adotadas pelos responsáveis pelo tratamento, durante a fase de desenvolvimento, para impedir ou limitar a recolha de dados pessoais utilizados para a formação, para reduzir a sua identificabilidade, para impedir a sua extração ou para fornecer garantias relativas à resistência de última geração aos ataques.

No que diz respeito à segunda e terceira questões, o parecer fornece considerações gerais que as AC devem ter em conta ao avaliar se os responsáveis pelo tratamento podem basear-se no interesse legítimo como base jurídica adequada para o tratamento realizado no contexto do desenvolvimento e da implantação de modelos de IA.

O parecer recorda que não existe uma hierarquia entre as bases jurídicas previstas no RGPD e que cabe aos responsáveis pelo tratamento identificar a base jurídica adequada para as suas atividades de tratamento. O parecer recorda, em seguida, o teste em três etapas que deve ser realizado ao avaliar a utilização do interesse legítimo como base jurídica, ou seja, 1) identificar o interesse legítimo prosseguido pelo responsável pelo tratamento ou por um terceiro; 2) analisar a necessidade do

tratamento para efeitos do(s) interesse(s) legítimo(s) prosseguido(s) (também referido(s) como «teste da necessidade»); e 3) avaliar se o(s) interesse(s) legítimo(s) não é(são) afetado(s) pelos interesses ou direitos e liberdades fundamentais dos titulares dos dados (também referido(s) como «teste de equilíbrio»).

No que diz respeito à primeira etapa, o parecer recorda que um interesse pode ser considerado legítimo se estiverem preenchidos os três critérios cumulativos seguintes: o interesse (1) é lícito; (2) está articulado de forma clara e precisa; e (3) é real e presente (ou seja, não é especulativo). Esse interesse pode abranger, por exemplo, o desenvolvimento de um modelo de IA - desenvolver o serviço de um agente de conversação para ajudar os utilizadores, ou a sua implantação - melhorar a deteção de ameaças num sistema de informação.

No que diz respeito à segunda etapa, o parecer recorda que a avaliação da necessidade implica considerar: 1) se a atividade de tratamento permitirá a prossecução do interesse legítimo; e 2) se não existe uma forma menos intrusiva de prosseguir esse interesse. Ao avaliar se a condição de necessidade está preenchida, as AC devem prestar especial atenção à quantidade de dados pessoais tratados e se é proporcional à prossecução do interesse legítimo em causa, também à luz do princípio da minimização dos dados.

No que respeita à terceira etapa, o parecer recorda que o teste de equilíbrio deve ser efetuado tendo em conta as circunstâncias específicas de cada caso. Em seguida, apresenta uma panorâmica dos elementos que as AC podem ter em conta ao avaliar se o interesse de um responsável pelo tratamento ou de um terceiro é derrogado pelos interesses, direitos e liberdades fundamentais dos titulares dos dados.

No âmbito da terceira etapa, o parecer destaca os riscos específicos para os direitos fundamentais que podem surgir quer na fase de desenvolvimento quer na fase de implantação dos modelos de IA. Esclarece igualmente que o tratamento de dados pessoais que ocorre durante as fases de desenvolvimento e implantação dos modelos de IA pode afetar os titulares dos dados de diferentes formas, o que pode ser positivo ou negativo. Para avaliar esse impacto, as AC podem considerar a natureza dos dados tratados pelos modelos, o contexto do tratamento e as possíveis consequências posteriores do tratamento.

Além disso, o parecer destaca o papel das expectativas razoáveis dos titulares dos dados no critério de equilíbrio. Tal pode ser importante devido à complexidade das tecnologias utilizadas nos modelos de IA e ao facto de poder ser difícil para os titulares dos dados compreender a variedade das suas utilizações potenciais, bem como as diferentes atividades de tratamento envolvidas. A este respeito, tanto as informações fornecidas aos titulares dos dados como o contexto do tratamento podem estar entre os elementos a considerar para avaliar se os titulares dos dados podem razoavelmente esperar que os seus dados pessoais sejam tratados. No que diz respeito ao contexto, tal pode incluir: se os dados pessoais estavam ou não disponíveis ao público, a natureza da relação entre o titular dos dados e o responsável pelo tratamento (e se existe uma ligação entre os dois), a natureza do serviço, o contexto em que os dados pessoais foram recolhidos, a fonte a partir da qual os dados foram recolhidos (ou seja, o sítio Web ou o serviço onde os dados pessoais foram recolhidos e as predefinições de privacidade que oferecem), as potenciais novas utilizações do modelo e se os titulares dos dados estão efetivamente cientes de que os seus dados pessoais estão, de todo, em linha.

O parecer recorda também que, quando os interesses, direitos e liberdades das pessoas em causa parecem sobrepor-se ao(s) interesse(s) legítimo(s) prosseguido(s) pelo responsável pelo tratamento ou por um terceiro, o responsável pelo tratamento pode considerar a introdução de medidas atenuantes para limitar o impacto do tratamento sobre essas pessoas. As medidas de atenuação não

devem ser confundidas com as medidas que o responsável pelo tratamento é legalmente obrigado a adotar de qualquer forma para assegurar o cumprimento do RGPD. Além disso, as medidas devem ser adaptadas às circunstâncias do caso e às caraterísticas do modelo de IA, incluindo a sua utilização prevista. A este respeito, o parecer fornece uma lista não exaustiva de exemplos de medidas atenuantes em relação à fase de desenvolvimento (também no que diz respeito à recolha de dados da Web) e à fase de implantação. As medidas de atenuação podem estar sujeitas a uma evolução rápida e devem ser adaptadas às circunstâncias do caso. Por conseguinte, continua a ser da responsabilidade das autoridades de controlo avaliar a adequação das medidas de atenuação aplicadas caso a caso.

No que diz respeito à quarta pergunta, o parecer recorda, em geral, que as AC dispõem de poderes discricionários para avaliar a(s) eventual(is) infração(ões) e escolher as medidas adequadas, necessárias e proporcionadas, tendo em conta as circunstâncias de cada caso individual. Em seguida, o parecer analisa três cenários.

No cenário 1, os dados pessoais são conservados no modelo de IA (o que significa que o modelo não pode ser considerado anónimo, conforme especificado na primeira pergunta) e são posteriormente tratados pelo mesmo responsável pelo tratamento (por exemplo, no contexto da implantação do modelo). O parecer afirma que a questão de saber se as fases de desenvolvimento e de implantação envolvem finalidades distintas (constituindo assim actividades de tratamento separadas) e em que medida a falta de base jurídica para a atividade de tratamento inicial afecta a legalidade do tratamento subsequente deve ser avaliada caso a caso, em função do contexto do caso.

No cenário 2, os dados pessoais são conservados no modelo e são tratados por outro responsável pelo tratamento no contexto da implantação do modelo. A este respeito, o Parecer refere que as AC devem ter em conta se o responsável pelo tratamento que utiliza o modelo realizou uma avaliação adequada, no âmbito das suas obrigações de prestação de contas para demonstrar a conformidade com o artigo 5.º, n.º 1, alínea a), e com o artigo 6.º do RGPD, a fim de verificar que o modelo de IA não foi desenvolvido através do tratamento ilícito de dados pessoais. Esta avaliação deve ter em conta, por exemplo, a fonte dos dados pessoais e se o tratamento na fase de desenvolvimento foi objeto da constatação de uma infração, em especial se tiver sido determinado por uma autoridade de controlo ou por um tribunal, e deve ser menos ou mais pormenorizado em função dos riscos suscitados pelo tratamento na fase de implantação.

No cenário 3, um responsável pelo tratamento trata ilegalmente dados pessoais para desenvolver o modelo de IA e, em seguida, assegura a sua anonimização, antes de o mesmo ou outro responsável pelo tratamento iniciar outro tratamento de dados pessoais no contexto da implantação. A este respeito, o parecer afirma que, se for possível demonstrar que o funcionamento subsequente do modelo de IA não implica o tratamento de dados pessoais, o CEPD considera que o RGPD não seria aplicável. Por conseguinte, a ilegalidade do tratamento inicial não deve afetar o funcionamento subsequente do modelo. Além disso, o CEPD considera que, quando os responsáveis pelo tratamento tratam subsequentemente os dados pessoais recolhidos durante a fase de implantação, depois de o modelo ter sido anonimizado, o RGPD seria aplicável em relação a essas operações de tratamento. Nestes casos, o Parecer considera que, no que se refere ao RGPD, a licitude do tratamento realizado na fase de implementação não deve ser afetada pela ilegalidade do tratamento inicial.

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 63.º e o artigo 64.º, n.º 2, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado «Regulamento Geral sobre a Proteção de Dados»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[1],

Tendo em conta os artigos 10.º e 22.º do seu Regulamento Interno,

Considerando o seguinte:

(1) O principal papel do Comité Europeu para a Proteção de Dados (a seguir designado por **«Comité»** ou **«RGPD»**) consiste em assegurar uma aplicação coerente do RGPD em todo o Espaço Económico Europeu (**«EEE»**). O artigo 64.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados determina que as autoridades de controlo (**«AC»**), o presidente do Comité ou a Comissão podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro do EEE, com vista a obter um parecer. O objetivo do presente parecer é analisar um assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro do EEE.

2) O parecer do Comité é aprovado nos termos do artigo 64.º, n.º 3, do RGPD, em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD, no prazo de oito semanas a contar da data em que o presidente e as autoridades de controlo competentes tenham decidido que o processo está completo. Por decisão do presidente, este prazo pode ser prorrogado por mais seis semanas, tendo em conta a complexidade do tema.

ADOTOU O PRESENTE PARECER:

1 Introdução

1.1 Resumo dos factos

1. Em 4 de setembro de 2024, a autoridade de controlo irlandesa (a «**AC irlandesa**» ou «**AC requerente**») solicitou ao CEPD que emitisse um parecer nos termos do artigo 64.º, n.º 2, do RGPD em relação aos modelos de IA e ao tratamento de dados pessoais («**o pedido**»).

2. O Presidente do Conselho de Administração e a AC IE consideraram o dossiê completo em 13 de setembro de 2024. No dia útil seguinte, 16 de setembro de 2024, o ficheiro foi transmitido pelo Secretariado do CEPD. Tendo em conta a complexidade da questão, a Presidente do Comité decidiu prorrogar o prazo legal, em conformidade com o artigo 64.º, n.º 3, do RGPD e o artigo 10.º, n.º 4, do Regulamento Interno.

[1] As referências a «Estados-Membros» no presente parecer devem ser entendidas como referências a «Estados-Membros do EEE». As referências à «União» no presente parecer devem ser entendidas como referências ao «EEE».

3. O pedido aborda determinados elementos da formação, atualização, desenvolvimento e funcionamento de modelos de IA em que os dados pessoais fazem parte do conjunto de dados relevante. A AC IE salienta que o pedido diz respeito a questões-chave que têm um elevado impacto nos titulares dos dados e nos responsáveis pelo tratamento no EEE e que, nesta fase, não existe uma posição harmonizada entre as AC nacionais[2]. A terminologia que será utilizada para efeitos do presente parecer é apresentada nas secções 2.2 e 2.3 infra.

4. A AC dinamarquesa colocou as perguntas seguintes:

Pergunta 1: Considera-se que o modelo de IA final, que foi formado utilizando dados pessoais, em todos os casos, não corresponde à definição de dados pessoais (tal como estabelecido no artigo 4.º, n.º 1, do RGPD)?

Em caso de resposta afirmativa à primeira questão:

i. Em que fase das operações de tratamento que conduzem a um modelo de IA é que os dados pessoais deixam de ser tratados?
   a) Como é que se pode demonstrar que o modelo de IA não processa dados pessoais?

ii. Existem fatores que possam fazer com que o funcionamento do modelo de IA final deixe de ser considerado anónimo?
   a) Em caso afirmativo, como podem ser demonstradas as medidas tomadas para atenuar, prevenir ou proteger contra estes fatores (de modo a assegurar que o modelo de IA não trata dados pessoais)?

Em caso de resposta negativa à primeira questão:

i. Quais são as circunstâncias em que isso pode acontecer?
   a) Em caso afirmativo, de que forma podem ser demonstradas as medidas tomadas para assegurar que o modelo de IA não está a tratar dados pessoais?

Pergunta 2: Quando um responsável pelo tratamento de dados se baseia em interesses legítimos como fundamento jurídico para o tratamento de dados pessoais para criar, atualizar e/ou desenvolver um modelo de IA, como deve esse responsável demonstrar a adequação dos interesses legítimos como fundamento jurídico, tanto em relação ao tratamento de dados de terceiros como de dados próprios?

i. Que considerações deve o responsável pelo tratamento ter em conta para garantir que os interesses das pessoas cujos dados pessoais estão a ser tratados são devidamente ponderados em relação aos interesses do responsável pelo tratamento no contexto de:
   a) Dados de terceiros

   b) Dados de primeira parte

Pergunta 3: Após a formação, quando um responsável pelo tratamento de dados se baseia em interesses legítimos como fundamento jurídico para o tratamento de dados pessoais efetuado no âmbito de um modelo de IA, ou de um sistema de IA do qual faz parte um modelo de IA, como deve o

[2]Pedido, p. 1.

responsável pelo tratamento demonstrar a adequação dos interesses legítimos como fundamento jurídico?

Pergunta 4: Se se verificar que um modelo de IA foi criado, atualizado ou desenvolvido utilizando dados pessoais tratados ilegalmente, qual é o impacto deste facto, se for caso disso, na legalidade do tratamento ou funcionamento continuado ou subsequente do modelo de IA, quer por si só, quer como parte de um sistema de IA, em que:

i. O modelo de IA, isoladamente ou como parte de um sistema de IA, está a processar dados pessoais?
ii. Nem o Modelo de IA, nem o Modelo de IA como parte de um Sistema de IA, estão a processar dados pessoais?

1.2 Quanto à admissibilidade do pedido de parecer nos termos do artigo 64.º, n.º 2, do RGPD

5. O artigo 64.º, n.º 2, do RGPD prevê que, em particular, as autoridades de controlo podem solicitar que qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro seja analisado pelo Comité com vista a obter um parecer.

6. A AC requerente dirigiu perguntas ao CEPD sobre os aspetos da proteção de dados no contexto dos modelos de IA. Especificou no pedido que, embora muitas organizações estejam agora a utilizar modelos de IA, incluindo grandes modelos linguísticos («**LLM**»), as suas operações, formação e utilização suscitam «*uma série de preocupações abrangentes em matéria de proteção de dados*»[3], que «*afetam os titulares dos dados em toda a UE/EEE*»[4].

7. O pedido levanta, no essencial, questões sobre (i) a aplicação do conceito de dados pessoais; (ii) o princípio da licitude, no que se refere especificamente à base jurídica do interesse legítimo, no contexto dos modelos de IA; bem como sobre (iii) as consequências do tratamento ilegal de dados pessoais na fase de desenvolvimento dos modelos de IA, sobre o subsequente tratamento ou funcionamento do modelo.

8. Por conseguinte, o Comité considera que este pedido diz respeito a um «*assunto de aplicação geral*» na aceção do artigo 64.º, n.º 2, do RGPD. Em particular, a questão prende-se com a interpretação e a aplicação do artigo 4.º, n.º 1, do artigo 5.º, n.º 1, alínea a), e do artigo 6.º do RGPD em relação ao tratamento de dados pessoais no desenvolvimento e na implantação de modelos de IA. Tal como salientado pela AC requerente, a aplicação destas disposições aos modelos de IA levanta questões sistémicas, abstratas e inovadoras[5]. O rápido desenvolvimento e implantação de modelos de IA por cada vez mais organizações levanta questões específicas e, tal como referido no pedido, *«o CEPD beneficiará muito de chegar a uma posição comum sobre as questões suscitadas pelo presente pedido, sendo essas questões centrais para o trabalho planeado do CEPD a curto e médio prazo»*[6]. Além disso, as tecnologias de IA criam muitas oportunidades e benefícios numa vasta gama de setores e atividades sociais. Além disso, o RGPD é um quadro jurídico que incentiva a inovação responsável. Daqui resulta

[3] Pedido, p. 1.
[4] Ibid.
[5] Pedido, p. 2.
[6] Pedido, p. 1. Tal como mencionado no Programa de Trabalho do CEPD para 2024-2025, adotado em 8 de outubro de 2024, disponível em https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, o CEPD planeia emitir, *inter alia*, orientações sobre anonimização, pseudonimização e raspagem de dados no contexto da IA generativa.

que existe um interesse geral em fazer esta avaliação sob a forma de um parecer do CEPD, a fim de assegurar a aplicação coerente de determinadas disposições do RGPD no contexto dos modelos de IA.

9. A segunda condição mencionada no artigo 64.º, n.º 2, do RGPD refere-se a um assunto «*que produza efeitos em mais do que um Estado-Membro*». O CEPD recorda que o termo «efeitos» deve ser interpretado *lato sensu* e, por conseguinte, não se limita simplesmente a efeitos jurídicos[7]. Uma vez que cada vez mais modelos de IA estão a ser treinados e utilizados por um número crescente de organizações no EEE, afetam um grande número de titulares de dados em todo o EEE, alguns dos quais já manifestaram preocupações à sua AC competente[8]. Por conseguinte, o CEPD considera que a questão suscitada pela AC requerente também preenche esta condição.

10. O pedido inclui uma fundamentação escrita sobre os antecedentes e as motivações para apresentar as questões ao Conselho de Administração, incluindo o quadro jurídico relevante. Por conseguinte, o Comité considera que o pedido é fundamentado em conformidade com o artigo 10.º, n.º 3, do Regulamento Interno do CEPD.

11. Nos termos do artigo 64.º, n.º 3, do RGPD, o CEPD não pode emitir um parecer se já tiver emitido um parecer sobre o assunto[9]. O CEPD não emitiu um parecer sobre o mesmo assunto e ainda não forneceu respostas às questões decorrentes do pedido.

12. Por estas razões, o Comité considera que o Pedido é admissível e que as questões dele decorrentes devem ser analisadas no presente parecer (o «**Parecer**») adotado nos termos do artigo 64.º, n.º 2, do RGPD.

2 Âmbito de aplicação e principais conceitos

2.1 Âmbito do parecer

13. O Comité concorda com a AC requerente de que, do ponto de vista da proteção de dados, o desenvolvimento e a implantação de modelos de IA levantam questões fundamentais em matéria de proteção de dados. As perguntas referem-se, nomeadamente, a: (i) quando e como um modelo de IA pode ser considerado «anónimo» (Pergunta 1 do pedido); (ii) como podem os responsáveis pelo tratamento demonstrar a adequação do interesse legítimo como base jurídica nas fases de desenvolvimento (Pergunta 2 do pedido) e implantação (Pergunta 3 do pedido); e (iii) se o tratamento ilícito de dados pessoais na fase de desenvolvimento tem consequências sobre a licitude do subsequente tratamento ou funcionamento do modelo de IA (Pergunta 4 do pedido).

14. O CEPD recorda que as autoridades de controlo são responsáveis pelo controlo da aplicação do RGPD e devem contribuir para a sua aplicação coerente em toda a União[10]. Por conseguinte, é da competência das AC investigar modelos de IA específicos e, ao fazê-lo, realizar avaliações caso a caso.

15. O presente Parecer estabelece um quadro para que as AC competentes avaliem casos específicos em que (algumas das) questões suscitadas no Pedido surgiriam. O presente parecer não pretende ser exaustivo, mas sim apresentar considerações gerais sobre a interpretação das disposições pertinentes,

[7]CEPD, documento interno 3/2019 sobre as orientações internas sobre o artigo 64.º, n.º 2, do RGPD, adotado em 8 de outubro de 2019, ponto 15, disponível em https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.
[8]Pedido, pp. 1-2.
[9] Artigo 64.º, n.º 3, do RGPD e artigo 10.º, n.º 4, do Regulamento Interno do CEPD.
[10]Artigo 51.º, n.º 1, do RGPD e artigo 51.º, n.º 2, do RGPD.

que as autoridades de controlo competentes devem ter na máxima conta no exercício dos seus poderes de investigação. Embora o presente parecer seja dirigido às AC competentes e diga respeito às suas atividades e poderes, não prejudica as obrigações dos responsáveis pelo tratamento e dos subcontratantes nos termos do RGPD. Em especial, de acordo com o princípio da responsabilidade consagrado no artigo 5.º, n.º 2, do RGPD, os responsáveis pelo tratamento são responsáveis por, e podem demonstrar o cumprimento de, todos os princípios relacionados com o seu tratamento de dados pessoais.

16. Nalguns casos, podem ser apresentados alguns exemplos no parecer, mas tendo em conta o âmbito alargado das questões incluídas no pedido, bem como os diferentes tipos de modelos de IA nele abrangidos, nem todos os cenários possíveis serão considerados no presente parecer. As tecnologias associadas aos modelos de IA estão sujeitas a uma rápida evolução; por conseguinte, as considerações do CEPD no presente parecer devem ser interpretadas à luz deste facto.

17. **O presente parecer não analisa as disposições seguintes, que podem ainda assim desempenhar um papel importante na avaliação dos requisitos de proteção de dados aplicáveis aos modelos de IA:**

- **Tratamento de categorias específicas de dados:** O CEPD recorda a proibição do artigo 9.º, n.º 1, do RGPD no que diz respeito ao tratamento de categorias especiais de dados e às exceções limitadas do artigo 9.º, n.º 2, do RGPD[11]. A este respeito, o Tribunal de Justiça da União Europeia (**«TJUE»**) esclareceu ainda que «*quando um conjunto de dados que contenha dados sensíveis e dados não sensíveis é [...] recolhido em bloco sem que seja possível separar os elementos de dados uns dos outros no momento da recolha, o tratamento desse conjunto de dados deve ser considerado proibido, na aceção do artigo 9.º, n.º 1, do RGPD, se contiver pelo menos um elemento de dados sensível e não se aplicar nenhuma das derrogações previstas no artigo 9.º, n.º 2, do referido regulamento*»[12]. Além disso, o TJUE salientou igualmente que *«para efeitos da aplicação da exceção prevista no artigo 9.º, n.º 2, alínea e), do RGPD, é importante verificar se o titular dos dados tinha pretendido, de forma explícita e através de uma ação afirmativa inequívoca, tornar os dados pessoais em questão acessíveis ao público em geral»* [13]. Estas considerações devem ser tidas em conta quando o tratamento de dados pessoais no contexto de modelos de IA envolve categorias especiais de dados.
- **Tomada de decisões automatizada, incluindo a definição de perfis**: As operações de tratamento realizadas no contexto de modelos de IA podem ser abrangidas pelo âmbito de aplicação do artigo 22.º do RGPD, que impõe obrigações adicionais aos responsáveis pelo tratamento e proporciona garantias adicionais aos titulares dos dados. O CEPD recorda, a este

[11]Ver também o relatório do CEPD sobre o trabalho realizado pelo grupo de trabalho ChatGPT, adotado em 23 de maio de 2024, ponto 18: «No que diz respeito ao tratamento de categorias especiais de dados pessoais, uma das exceções do artigo 9.º, n.º 2, deve ser igualmente aplicável para que o tratamento seja lícito. *Em princípio, uma destas exceções pode ser o artigo 9.º, n.º 2, alínea e), do RGPD. No entanto, o simples facto de os dados pessoais serem acessíveis ao público não implica que «o titular dos dados tenha manifestamente tornado públicos esses dados» [...]*».

[12] Acórdão do TJUE de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), parágrafo 89.

[13] Acórdão do TJUE de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), parágrafo 77.

respeito, as suas orientações sobre a tomada automatizada de decisões individuais e a definição de perfis para efeitos do Regulamento (UE) 2016/679[14].

- **Compatibilidade das finalidades**: O artigo 6.º, n.º 4, do RGPD prevê, para certas bases jurídicas, critérios que um responsável pelo tratamento deve ter em conta para determinar se o tratamento para outra finalidade é compatível com a finalidade para a qual os dados pessoais são inicialmente recolhidos. Esta disposição pode ser relevante no contexto do desenvolvimento e da implantação de modelos de IA e a sua aplicabilidade deve ser avaliada pelas autoridades de controlo.

- **Avaliações de impacto sobre a proteção de dados** («**AIPD**») (artigo 35.º do RGPD): As avaliações de impacto da proteção de dados são um elemento importante da responsabilização, em que o tratamento no contexto dos modelos de IA é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares[15].

- **Princípio da proteção de dados desde a conceção** (artigo 25.º, n.º 1, do RGPD): A proteção de dados desde a conceção é uma salvaguarda essencial que deve ser avaliada pelas AC no contexto do desenvolvimento e da implantação de um modelo de IA.

2.2 Noções-chave

18. A título de observação preliminar, o CEPD pretende prestar esclarecimentos sobre a terminologia e os conceitos que utiliza ao longo do presente parecer, e apenas para efeitos do presente parecer:

- «**Dados de primeira parte»**refere-se a dados pessoais que o responsável pelo tratamento recolheu junto dos titulares dos dados.

- «**Dados de terceiros**», os dados pessoais que os responsáveis pelo tratamento não obtiveram dos titulares dos dados, mas recolheram ou receberam de terceiros, por exemplo, de um corretor de dados ou recolhidos através de recolha de material na Web.

- «**Web scraping**» é uma técnica comummente utilizada para recolher informações de fontes em linha publicamente disponíveis. As informações retiradas, por exemplo, de serviços como canais de notícias, redes sociais, debates de fóruns e sítios Web pessoais podem conter dados pessoais.

- O pedido refere-se ao **«ciclo de vida» dos modelos de IA**, bem como a várias fases relativas, nomeadamente, à «criação», ao «desenvolvimento», à «formação», à «atualização», ao «aperfeiçoamento», à «operação» ou à «pós-formação» dos modelos de IA. O CEPD reconhece que, dependendo das circunstâncias, essas fases podem ter lugar no desenvolvimento e na implantação de modelos de IA e podem incluir o tratamento de dados pessoais para várias finalidades de tratamento. No entanto, para efeitos do presente parecer, o CEPD considera importante simplificar a categorização das fases suscetíveis de ocorrer. Por conseguinte, para efeitos do presente parecer, o CEPD refere-se à «**fase de desenvolvimento**» e à «**fase de implantação**». O desenvolvimento de um modelo de IA abrange todas as fases antes de qualquer

[14] Grupo de Trabalho do Artigo 29.º (**«WP29»**) Orientações sobre a tomada de decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento 2016/679, tal como revistas e adoptadas pela última vez em 6 de fevereiro de 2018, aprovadas pelo CEPD em 25 de maio de 2018. Ver também o acórdão do TJUE de 7 de dezembro de 2023, Processo C-634/21, *SCHUFA Holding e outros* (ECLI:EU:C:2023:957).

[15] WP29, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, revistas e adotadas em 4 de outubro de 2017, aprovadas pelo CEPD em 25 de maio de 2018

implantação do modelo de IA e inclui, nomeadamente, o desenvolvimento do código, a recolha de dados pessoais de formação, o pré-processamento dos dados pessoais de formação e a formação. A implantação de um modelo de IA abrange todas as fases relacionadas com a utilização de um modelo de IA e pode incluir quaisquer operações realizadas após a fase de desenvolvimento. O CEPD continua ciente da variedade de casos de utilização e das suas potenciais consequências em termos de tratamento de dados pessoais; assim, as AC devem considerar se as observações apresentadas no presente parecer são relevantes para o tratamento que estão a avaliar.

- O CEPD salienta igualmente que, quando necessário, o termo «**formação**» se refere à parte da fase de desenvolvimento em que os modelos de IA aprendem com os dados para desempenharem as funções que lhes foram atribuídas (tal como explicado na secção seguinte do presente parecer).
- A noção e o âmbito de aplicação dos **modelos de IA**, tal como entendidos pelo CEPD para efeitos do presente parecer, são especificados mais pormenorizadamente na secção específica que se segue.

2.3 Modelos de IA no contexto do Parecer

19. O Regulamento Inteligência Artificial da UE («**AI Act**»)[16] define um «sistema de IA» como «*um sistema baseado em máquinas concebido para funcionar com níveis variáveis de autonomia e que pode apresentar adaptabilidade após a implantação e que, para objetivos explícitos ou implícitos, infere, a partir dos dados que recebe, como gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais*» [17]. O considerando (12) do Regulamento Inteligência Artificial explica ainda a noção de «sistema de IA». Por conseguinte, uma característica principal dos sistemas de IA é a sua capacidade de fazer inferências. As técnicas que permitem a inferência durante a construção de um sistema de IA incluem a aprendizagem automática e abordagens baseadas na lógica e no conhecimento.

20. Por outro lado, os «modelos de IA» são definidos apenas indiretamente no Regulamento Inteligência Artificial: «*Embora os modelos de IA sejam componentes essenciais dos sistemas de IA, não constituem sistemas de IA por si só. Os modelos de IA requerem a adição de outros componentes, como, por exemplo, uma interface de utilizador, para se tornarem sistemas de IA. Os modelos de IA são normalmente integrados e fazem parte de sistemas de IA*»[18].

21. O CEPD entende que a definição de um modelo de IA proposta no pedido é mais restrita do que a do Regulamento IA, uma vez que se refere a «modelo de IA» como «*para abranger o produto resultante dos mecanismos de formação que são aplicados a um conjunto de dados de formação, no contexto da Inteligência Artificial, da Aprendizagem Automática, da Aprendizagem Profunda ou de outros contextos de processamento relacionados*» e especifica ainda que «*O termo aplica-se a modelos de IA que se destinam a ser submetidos a formação adicional, afinação e/ou desenvolvimento, bem como a modelos de IA que não são*.»[19]

[16] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).
[17] Ver artigo 3.º, n.º 1, do Regulamento IA.
[18] Considerando 97 do Regulamento IA.
[19] Pedido, p. 3.

22. Nessa base, o CEPD adotou o presente parecer no pressuposto de que um sistema de IA dependerá de um modelo de IA para cumprir o seu objetivo pretendido, incorporando o modelo num quadro mais vasto (por exemplo, um sistema de IA para serviço ao cliente pode utilizar um modelo de IA treinado com base em dados históricos de conversa para fornecer respostas a consultas dos utilizadores).

23. Além disso, os modelos de IA (ou «**modelos**) relevantes para o presente parecer são os desenvolvidos através de um processo de formação. Este processo de formação faz parte da fase de desenvolvimento, em que os modelos aprendem com os dados para desempenhar a tarefa pretendida. Por conseguinte, o processo de formação exige um conjunto de dados a partir do qual o modelo identificará e «aprenderá» padrões. Nestes casos, o modelo utilizará diferentes técnicas para construir uma representação do conhecimento extraído do conjunto de dados de treino. É nomeadamente o caso da aprendizagem automática.

24. Na prática, qualquer modelo de IA é um algoritmo, cujo funcionamento é determinado por um conjunto de elementos. Por exemplo, os modelos de aprendizagem profunda assumem frequentemente a forma de uma rede neuronal com múltiplas camadas constituídas por nós ligados por bordos com pesos, que são ajustados durante a formação para aprender as relações entre entradas e saídas. As características de um modelo simples de aprendizagem profunda seriam as seguintes: (i) o tipo e a dimensão de cada camada, (ii) o peso atribuído a cada borda (por vezes designados «parâmetros»), (iii) as funções de ativação[20] entre camadas e, possivelmente, (iv) outras operações que possam ocorrer entre camadas. Por exemplo, ao treinar um modelo simples de aprendizagem profunda para a classificação de imagens, os dados de entrada (os «**pixels de imagem**») serão associados aos resultados, e os pesos podem ser ajustados, de modo a produzir o resultado certo na maior parte do tempo.

25. Outros exemplos de modelos de aprendizagem profunda incluem os instrumentos de aprendizagem ao longo da vida e a IA generativa, que são utilizados, por exemplo, para gerar conteúdos semelhantes aos humanos e criar novos dados.

26. **Com base nas considerações acima expostas, em consonância com o pedido, o âmbito do presente parecer abrange apenas o subconjunto de modelos de IA que são o resultado de uma formação desses modelos com dados pessoais.**

3 Sobre o mérito do pedido

3.1 Sobre a natureza dos modelos de IA em relação à definição de dados pessoais

27. O artigo 4.º, n.º 1, do RGPD define os dados pessoais como «*qualquer informação relativa a uma pessoa singular identificada ou identificável*» (ou seja, o titular dos dados). Além disso, o considerando 26 do RGPD prevê que os princípios de proteção de dados não devem ser aplicáveis às informações anónimas, nomeadamente às informações que não digam respeito a uma pessoa singular identificada ou identificável, tendo em conta «*todos os meios razoavelmente suscetíveis de serem utilizados*» pelo responsável pelo tratamento ou por outra pessoa. Isto implica: i) dados que nunca tenham estado relacionados com uma pessoa identificada ou identificável; e ii) dados pessoais que tenham sido tornados anónimos de tal forma que o titular dos dados não seja ou deixe de ser identificável.

[20] Ou seja, funções que calculam, com base nas entradas e nos pesos, a saída de um nó neural que será depois enviada para a camada seguinte da rede neural.

28. Por conseguinte, a pergunta 1[21] do pedido pode ser respondida analisando se um modelo de IA resultante de uma formação que envolva o tratamento de dados pessoais deve, em todos os casos, ser considerado anónimo. Com base na formulação da pergunta, o CEPD referir-se-á, nesta secção, ao processo de «formação» de um modelo de IA.

29. Antes de mais, o CEPD gostaria de apresentar as seguintes considerações gerais. Os modelos de IA, independentemente de serem ou não treinados com dados pessoais, são geralmente concebidos para fazer previsões ou tirar conclusões, ou seja, são concebidos para inferir. Além disso, os modelos de IA treinados com dados pessoais são frequentemente concebidos para fazer inferências sobre indivíduos diferentes daqueles cujos dados pessoais foram utilizados para treinar o modelo de IA. No entanto, alguns modelos de IA são especificamente concebidos para fornecer dados pessoais relativos a indivíduos cujos dados pessoais foram utilizados para treinar o modelo, ou de alguma forma para disponibilizar esses dados. Nestes casos, esses modelos de IA incluirão intrinsecamente (e normalmente necessariamente) informações relativas a uma pessoa singular identificada ou identificável, pelo que envolverão o tratamento de dados pessoais. Por conseguinte, estes tipos de modelos de IA não podem ser considerados anónimos. Seria o caso, por exemplo, (i) de um modelo generativo aperfeiçoado com base nas gravações de voz de um indivíduo para imitar a sua voz; ou (ii) de qualquer modelo concebido para responder com dados pessoais da formação quando lhe são pedidas informações sobre uma pessoa específica.

30. Com base nas considerações anteriores, ao responder à pergunta 1 do pedido, o CEPD centra-se na situação dos modelos de IA que não são concebidos para fornecer dados pessoais relacionados com os dados de formação.

31. O CEPD considera que, mesmo que um modelo de IA não tenha sido intencionalmente concebido para produzir informações relativas a uma pessoa singular identificada ou identificável a partir dos dados de treino, as informações do conjunto de dados de treino, incluindo dados pessoais, podem continuar a ser «absorvidas» nos parâmetros do modelo, nomeadamente representadas através de objetos matemáticos. Podem ser diferentes dos pontos de dados de treino originais, mas podem ainda reter a informação original desses dados, que pode, em última análise, ser extraída ou obtida de outra forma, direta ou indiretamente, a partir do modelo. Sempre que as informações relativas a pessoas identificadas ou identificáveis cujos dados pessoais foram utilizados para treinar o modelo possam ser obtidas a partir de um modelo de IA com meios razoavelmente susceptíveis de serem utilizados, pode concluir-se que esse modelo não é anónimo.

32. A este respeito, o pedido refere que «*As publicações de investigação existentes destacam algumas vulnerabilidades potenciais que podem existir nos modelos de IA e que podem resultar no tratamento de dados pessoais,[22] bem como o tratamento de dados pessoais que pode ocorrer quando os modelos são implantados para utilização com outros dados, quer através de interfaces de programação de aplicações (**«APIs»**) quer de interfaces «prompt»*»[23].

[21] «*Considera-se que o modelo final de IA, que foi treinado utilizando dados pessoais, não corresponde, em todos os casos, à definição de dados pessoais (tal como estabelecido no artigo 4.º, n.º 1, do RGPD)?*»
[22] Tais como os ataques de inferência de membros (OWASP) e os ataques de inversão de modelos (OWASP & Veale et al, 2018).
[23] Pedido, p. 1-2.

33. Na mesma linha, a investigação sobre a extração de dados de formação é particularmente dinâmica[24]. Mostra que é possível, em alguns casos, utilizar meios razoavelmente susceptíveis de extrair dados pessoais de alguns modelos de IA, ou simplesmente obter acidentalmente dados pessoais através de interações com um modelo de IA (por exemplo, como parte de um sistema de IA). Os esforços contínuos de investigação neste domínio ajudarão a avaliar melhor os riscos residuais da regurgitação[25] e da extração de dados pessoais num determinado caso.

34. **Com base nas considerações anteriores, o CEPD considera que os modelos de IA treinados em dados pessoais não podem, em todos os casos, ser considerados anónimos. Em vez disso, a determinação do anonimato de um modelo de IA deve ser avaliada caso a caso, com base em critérios específicos.**

3.2 Sobre as circunstâncias em que os modelos de IA podem ser considerados anónimos e a respetiva demonstração

35. Relativamente à pergunta 1 do pedido[26], solicita-se ao CEPD que esclareça as circunstâncias em que um modelo de IA, que foi treinado utilizando dados pessoais, pode ser considerado anónimo. No que diz respeito à pergunta 1, ponto i), alínea a), do pedido[27], o CEPD é solicitado a esclarecer que provas e/ou documentação as AC devem ter em conta ao avaliar se um modelo de IA é anónimo.

3.2.1 Considerações gerais sobre a anonimização no contexto atual

36. A utilização da expressão «*qualquer informação*» na definição de «*dados pessoais*» no artigo 4.º, n.º 1, do RGPD reflete o objetivo de atribuir um âmbito alargado a esse conceito, que engloba todos os tipos de informações desde que «*diga respeito*» ao titular dos dados, que são identificados ou podem ser identificados direta ou indiretamente.

37. As informações podem dizer respeito a uma pessoa singular mesmo que sejam tecnicamente organizadas ou codificadas (por exemplo, num formato exclusivamente legível por máquina, seja ele exclusivo ou aberto) de uma forma que não torne imediatamente visível a relação com essa pessoa singular. Nesses casos, as aplicações de software podem ser utilizadas para identificar, reconhecer e extrair facilmente dados específicos. Isto é particularmente verdade no caso dos modelos de IA em que os parâmetros representam relações estatísticas entre os dados da formação e em que pode ser

[24] Ver, a este respeito, por exemplo: (i) Veale M., Binns R., Edwards L., 2018, *Algoritmos que se lembram: ataques de inversão de modelos e lei de proteção de dados*. Phil. TRANS. R. Soc. A 376: 20180083, disponível em http://dx.doi.org/10.1098/rsta.2018.0083; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, June 20, 2022, Seoul, Republic of Korea, disponível em https://dl.acm.org/doi/abs/10.1145/3531146.3534642; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, janeiro de 2024, National Institute of Standards and Technology, disponível em https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15 Jun 2021, disponível em https://arxiv.org/pdf/2012.07805; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 de outubro de 2015, disponível em https://dl.acm.org/doi/abs/10.1145/2810103.2813677; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18 Apr 2020, disponível em https://arxiv.org/pdf/1911.07135.

[25] Para um sistema de IA baseado na IA generativa, a regurgência corresponde à situação em que os resultados estariam diretamente relacionados com dados de formação.

[26] «*quais são as circunstâncias em que tal pode ocorrer?*»

[27] «*Em caso afirmativo, como podem ser demonstradas as medidas que foram tomadas para garantir que o modelo de IA não está a processar dados pessoais?*»

possível extrair dados pessoais exatos ou inexatos (porque estatisticamente inferidos), quer diretamente a partir das relações entre os dados incluídos no modelo, quer através da consulta desse modelo.

38. Uma vez que os modelos de IA não contêm normalmente registos que possam ser diretamente isolados ou ligados, mas sim parâmetros que representam relações probabilísticas entre os dados contidos no modelo, pode ser possível inferir[28] informações a partir do modelo, como a inferência de filiação, em cenários realistas. Por conseguinte, para que uma AC concorde com o responsável pelo tratamento de que um determinado modelo de IA pode ser considerado anónimo, deve verificar, pelo menos, se recebeu provas suficientes de que, com meios razoáveis: (i) os dados pessoais relacionados com os dados de formação não podem ser extraídos[29] a partir do modelo; e (ii) qualquer resultado obtido aquando da consulta do modelo não diz respeito aos titulares dos dados cujos dados pessoais foram utilizados para treinar o modelo.

39. As AC devem ter em conta três elementos na avaliação do cumprimento destas condições.

40. Em primeiro lugar, as AC devem ter em conta os elementos identificados nos pareceres mais recentes do GT29 e/ou nas orientações do CEPD sobre o assunto. No que diz respeito à anonimização à data do presente parecer, as AC devem ter em conta os elementos incluídos no Parecer 05/2014 do GT29 sobre técnicas de anonimização (o **«Parecer 05/2014 do GT29»**), que estabelece que, se não for possível separar, ligar e inferir informações do conjunto de dados supostamente anónimo, os dados podem ser considerados anónimos[30]. Também refere que, «*sempre que uma proposta não cumpra um dos*

[28] (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, disponível em https://arxiv.org/abs/2112.03570;
(ii) Creţu A.M, Guépin F., e De Montjoye Y.A, *Ataques de inferência da correlação contra modelos de aprendizagem automática*. J. Environ. Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 disponível em https://www.science.org/doi/10.1126/sciadv.adj9260;
(iii) Dana L., Pydi M. S., Chevaleyre Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15 November 2024, disponível em: https://arxiv.org/abs/2411.10115;
(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Levantamento em apoio da inferência probabilística com preservação da privacidade*. Künstl Intell, 13 de junho de 2024, disponível em https://doi.org/10.1007/s13218-024-00851-y:
(v) HU H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, disponível em https://github.com/HongshengHu/membership-inference-machine-learning-literature:
(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28 November 2023, disponível em: https://arxiv.org/abs/2311.17035;
(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 de março de 2017, disponível em https://arxiv.org/abs/1610.05820;
(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond memorisation: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6 de maio de 2024, disponível em https://arxiv.org/abs/2310.07298;
(ix) Wu F., Cui L., Yao S., Yu S., *InferenceAttacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Diretions* arXiv:2406.02027v1 [cs.LG], 27 de junho de 2024, disponível em https://arxiv.org/abs/2406.02027v1;
(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29 de setembro de 2024, disponível em https://arxiv.org/abs/2409.19798;
(xi) Zhou Z., Xiang J., Chen C., and Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL] 5 Nov 2023, disponível em: https://arxiv.org/abs/2308.15727.

[29] A extração inclui, em particular, o caso em que os dados pessoais são deduzidos do próprio modelo de IA, com pouca ou nenhuma utilização das interfaces de consulta.

[30] Parecer 05/2014 do GT29, página 24.

critérios, deve ser efetuada uma avaliação exaustiva dos riscos de identificação»[31]. **Dada a probabilidade de extração e de inferência acima referida, o CEPD considera que é muito provável que os modelos de IA exijam uma avaliação tão exaustiva dos riscos de identificação.**

41. Em segundo lugar, esta avaliação deve ser efetuada tendo em conta «*todos os meios razoavelmente suscetíveis de serem utilizados*» pelo responsável pelo tratamento ou por outra pessoa para identificar as pessoas[32], e a determinação desses meios deve basear-se em fatores objetivos, tal como explicado no considerando 26 do RGPD, que podem incluir:
    a. as caraterísticas dos próprios dados de formação, o modelo de IA e o procedimento de formação[33];
    b. o contexto em que o modelo de IA é libertado e/ou processado[34];
    c. as informações adicionais que permitiriam a identificação e que podem estar disponíveis para a pessoa em causa;
    d. os custos e o tempo de que a pessoa necessitará para obter essas informações adicionais (caso não estejam já disponíveis)[35]; e
    e. a tecnologia disponível no momento do processamento, bem como os desenvolvimentos tecnológicos[36].

42. Em terceiro lugar, as AC devem considerar se os responsáveis pelo tratamento avaliaram o risco de identificação pelo responsável pelo tratamento e por diferentes tipos de *«outras pessoas»*, incluindo terceiros não intencionais que acedem ao modelo de IA, tendo igualmente em conta se se pode razoavelmente considerar que conseguem obter acesso ou tratar os dados em questão.

43. **Em suma, o CEPD considera que, para que um modelo de IA seja considerado anónimo, utilizando meios razoáveis, tanto (i) a probabilidade de extração direta (incluindo probabilística) de dados pessoais relativos a indivíduos cujos dados pessoais foram utilizados para treinar o modelo; como (ii) a probabilidade de obter, intencionalmente ou não, esses dados pessoais a partir de consultas, devem ser insignificantes[37] para qualquer titular de dados**. **Por defeito, as AC devem considerar que os modelos de IA são suscetíveis de exigir uma avaliação exaustiva da probabilidade de identificação para chegar a uma conclusão sobre a sua possível natureza anónima. Esta probabilidade deve ser avaliada tendo em conta «*todos os meios razoavelmente suscetíveis de serem utilizados*» pelo responsável pelo tratamento ou por outra pessoa, e deve também ter em conta a (re)utilização ou divulgação não intencional do modelo.**

[31] Parecer 05/2014 do GT29, página 24.

[32] Acórdão do TJUE de 19 de outubro de 2016, Processo C-582/14, *Breyer v Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), parágrafo 43.

[33] Isto inclui caraterísticas como a singularidade dos registos nos dados de formação, a precisão da informação, a agregação, a aleatorização e, em particular, a forma como estas afetam a vulnerabilidade à identificação.

[34] Tal inclui elementos contextuais, tais como limitar o acesso apenas a algumas pessoas e salvaguardas jurídicas.

Acórdão do[35] TJUE de 7 de março de 2024, processo C-479/22 P*, OC/Comissão Europeia* (ECLI:EU:C:2024:215), ponto 50.

Acórdão do[36] TJUE de 7 de março de 2024, processo C-479/22 P*, OC/Comissão Europeia* (ECLI:EU:C:2024:215), ponto 50.

[37] Acórdão do TJUE de 19 de outubro de 2016, Processo C-582/14, *Breyer contra Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), n.º 46, e acórdão do TJUE de 7 de março de 2024, Processo C-479/22 P, *OC contra Comissão Europeia* (ECLI:EU:C:2024:215), n.º 51.

3.2.2 Elementos para avaliar a probabilidade residual de identificação

44. Embora possam ser tomadas medidas tanto nas fases de desenvolvimento como de implantação, a fim de reduzir a probabilidade de obtenção de dados pessoais a partir de um modelo de IA, a avaliação do anonimato de um modelo de IA deve também considerar o acesso direto ao modelo.

45. Além disso, as AC devem avaliar, caso a caso, se as medidas aplicadas pelo responsável pelo tratamento para assegurar e provar que um modelo de IA é anónimo são adequadas e eficazes.

46. Em particular, a conclusão da avaliação de uma AC pode diferir entre um modelo de IA disponível ao público, que é acessível a um número desconhecido de pessoas com uma gama desconhecida de métodos para tentar extrair dados pessoais, e um modelo de IA interno apenas acessível aos funcionários. Embora, em ambos os casos, as AC devam verificar se os responsáveis pelo tratamento cumpriram a sua obrigação de responsabilização nos termos do artigo 5.º, n.º 2, e do artigo 24.º do RGPD, os «*meios razoavelmente suscetíveis de serem utilizados*» por outras pessoas podem ter impacto na gama e na natureza dos possíveis cenários a considerar. Por conseguinte, dependendo do contexto de desenvolvimento e implantação do modelo, as AC podem considerar diferentes níveis de testes e resistência a ataques.

47. A este respeito, o CEPD apresenta a seguir uma lista não prescritiva e não exaustiva de possíveis elementos que podem ser considerados pelas AC ao avaliarem a alegação de anonimato de um responsável pelo tratamento de dados. Podem ser possíveis outras abordagens se oferecerem um nível de proteção equivalente, nomeadamente tendo em conta o estado da técnica.

48. A presença ou ausência dos elementos a seguir enumerados não é um critério conclusivo para avaliar o anonimato de um modelo de IA.

3.2.2.1 Conceção do modelo de IA

49. No que diz respeito à conceção de modelos de IA, as AC devem avaliar as abordagens adotadas pelos responsáveis pelo tratamento durante a fase de desenvolvimento. A este respeito, há que ter em conta a aplicação e a eficácia de quatro áreas-chave (a seguir identificadas).

Seleção de fontes

50. A primeira área de avaliação consiste em examinar a seleção das fontes utilizadas para treinar o modelo de IA. Isto inclui uma avaliação, pelas AC, de quaisquer medidas tomadas para evitar ou limitar a recolha de dados pessoais, incluindo, entre outras coisas, (i) a adequação dos critérios de seleção; (ii) a relevância e adequação das fontes escolhidas tendo em conta o(s) objetivo(s) pretendido(s); e (iii) se foram excluídas fontes inadequadas.

Preparação e minimização de dados

51. A segunda área de avaliação diz respeito à preparação de dados para a fase de formação. As avaliações de impacto devem examinar, em particular i) se foi considerada a utilização de dados anónimos e/ou pessoais que tenham sido pseudonimizados; e ii) caso tenha sido decidido não utilizar essas medidas, as razões para esta decisão, tendo em conta a finalidade prevista; iii) as estratégias e técnicas de minimização de dados utilizadas para limitar o volume de dados pessoais incluídos no processo de formação; e iv) quaisquer processos de filtragem de dados aplicados antes da formação do modelo destinados a eliminar dados pessoais irrelevantes.

Escolhas metodológicas relativamente à formação

52. A terceira área de avaliação diz respeito à seleção de métodos robustos no desenvolvimento de modelos de IA. A AC deve avaliar as escolhas metodológicas que possam reduzir ou eliminar significativamente a identificabilidade, incluindo, entre outros: se essa metodologia utiliza métodos de

regularização para melhorar a generalização do modelo e reduzir a sobreadaptação; e, fundamentalmente, ii) se o responsável pelo tratamento aplicou técnicas adequadas e eficazes de preservação da privacidade (por exemplo, privacidade diferencial).

Medidas relativas aos resultados do modelo

53. A última área de avaliação diz respeito a quaisquer métodos ou medidas adicionados ao próprio modelo de IA que possam não ter impacto no risco de extração direta de dados pessoais para o modelo por qualquer pessoa que o aceda diretamente, mas que possam reduzir a probabilidade de obtenção de dados pessoais relacionados com os dados de formação a partir de consultas.

3.2.2.2 Análise do modelo de IA

54. Para que as AC avaliem a solidez do modelo de IA concebido no que diz respeito à anonimização, um primeiro passo consiste em assegurar que a conceção foi desenvolvida conforme planeado e está sujeita a uma governação de engenharia eficaz. A AC deve avaliar se os responsáveis pelo tratamento realizaram quaisquer auditorias (internas ou externas) baseadas em documentos que incluam uma avaliação das medidas escolhidas e do seu impacto, a fim de limitar a probabilidade de identificação. Isto pode incluir a análise de relatórios de revisões de código, bem como uma análise teórica que documente a adequação das medidas escolhidas para reduzir a probabilidade de reidentificação do modelo em causa.

3.2.2.3 Testes de modelos de IA e resistência a ataques

55. Por último, as AC devem ter em consideração o âmbito, a frequência, a quantidade e a qualidade dos testes que o controlador efetuou no modelo. Em particular, as AC devem ter em conta que a realização de testes bem sucedidos que abranjam ataques amplamente conhecidos e de última geração só pode ser uma prova da resistência a esses ataques. Até à data do presente parecer, tal poderia incluir, entre outros, testes estruturados contra: (i) inferência de atributos e associações; (ii) exfiltração; (iii) regurgitação de dados de treino; (iv) inversão de modelos; ou (v) ataques de reconstrução.

3.2.2.4 Documentação

56. Os artigos 5.º, 24.º, 25.º e 30.º do RGPD e, nos casos de risco provavelmente elevado para os direitos e liberdades dos titulares dos dados, o artigo 35.º do RGPD, exigem que os responsáveis pelo tratamento documentem adequadamente as suas operações de tratamento. Isto também se aplica a qualquer tratamento que inclua o treino de um modelo de IA, mesmo que o objetivo do tratamento seja a anonimização. As AC devem ter em conta essa documentação e qualquer avaliação regular dos riscos consequentes do tratamento efetuado pelos responsáveis pelo tratamento, uma vez que são passos fundamentais para demonstrar que os dados pessoais não são tratados.

57. **O CEPD considera que as AC devem ter em conta a documentação sempre que seja necessário avaliar uma alegação de anonimato relativamente a um determinado modelo de IA. O CEPD observa que, se uma AC não puder confirmar, após avaliar a alegação de anonimato, nomeadamente à luz da documentação, que foram tomadas medidas eficazes para anonimizar o modelo de IA, a AC estaria em condições de considerar que o responsável pelo tratamento não cumpriu as suas obrigações de responsabilização nos termos do artigo 5.º, n.º 2, do RGPD. Por conseguinte, deve também ser considerada a conformidade com outras disposições do RGPD.**

58. Idealmente, as AC devem verificar se a documentação do responsável pelo tratamento inclui:

    a. quaisquer informações relacionadas com as AIPD, incluindo quaisquer avaliações e decisões que determinem que uma AIPD não era necessária;

b. qualquer conselho ou feedback fornecido pelo responsável pela proteção de dados («**RPD**») (quando foi - ou deveria ter sido - nomeado um RPD);

c. informações sobre as medidas técnicas e organizativas tomadas durante a conceção do modelo de IA para reduzir a probabilidade de identificação, incluindo o modelo de ameaça e as avaliações de risco em que se baseiam essas medidas. Tal deve incluir as medidas específicas para cada fonte de conjuntos de dados de formação, incluindo os URL das fontes pertinentes e descrições das medidas tomadas (ou já tomadas por terceiros fornecedores de conjuntos de dados);

d. as medidas técnicas e organizativas adotadas em todas as fases ao longo do ciclo de vida do modelo, que contribuíram para, ou verificaram, a falta de dados pessoais no modelo;

e. a documentação que demonstra a resistência teórica do modelo de IA às técnicas de reidentificação, bem como os controlos concebidos para limitar ou avaliar o êxito e o impacto dos principais ataques (regurgitação, ataques de inferência de filiação, exfiltração, etc.). Estas medidas podem incluir, em especial: (i) o rácio entre a quantidade de dados de treino e o número de parâmetros no modelo, incluindo a análise do seu impacto no modelo[38]; (ii) métricas sobre a probabilidade de reidentificação com base no atual estado da arte; (iii) relatórios sobre a forma como o modelo foi testado (por quem, quando, como e em que medida) e (iv) os resultados dos testes;

f. a documentação fornecida ao(s) responsável(is) pelo tratamento que aplica o modelo e/ou aos titulares dos dados, em especial a documentação relacionada com as medidas tomadas para reduzir a probabilidade de identificação e com os possíveis riscos residuais.

3.3 Sobre a adequação do interesse legítimo como base jurídica para o tratamento de dados pessoais no contexto do desenvolvimento e da implantação de modelos de IA

59. Para responder às perguntas 2 e 3 do pedido, o CEPD apresentará, em primeiro lugar, observações gerais sobre alguns aspetos importantes que as AC devem ter em conta, independentemente da base jurídica para o tratamento, ao avaliar a forma como os responsáveis pelo tratamento podem demonstrar a conformidade com o RGPD no contexto dos modelos de IA. O CEPD, com base nas Orientações 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD[39], analisará em seguida as três etapas exigidas pela avaliação do interesse legítimo no contexto do desenvolvimento e da implantação de modelos de IA.

3.3.1 Observações gerais

60. O CEPD recorda que o RGPD não estabelece qualquer hierarquia entre as diferentes bases jurídicas previstas no artigo 6.º, n.º 1, do RGPD[40].

[38] Ricciato F., *A Cautionary Reflection on (pseudo-) Synthetic Data from Deep Learning on Personal Data*, Privacy in Statistical Databases Conference (PSD 2024), Antibes, França, setembro de 2024, diapositivos disponíveis em: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf e Belkin M., Hsu D., Ma S., &Mandal S. (2019), *Reconciling modern Mache-learning practice and the clássic bias-variance trade-off*. Atas da Academia Nacional das Ciências, 24 de julho de 2019, 116 (32) 15849-15854, disponível em: https://www.pnas.org/doi/10.1073/pnas.1903070116

[39] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024.

[40] Ibid, n.º 1.

61. O artigo 5.º do RGPD estabelece os princípios relativos ao tratamento de dados pessoais. O CEPD destaca os que são significativos para o presente parecer e que devem, pelo menos, ser considerados pelas AC ao avaliarem modelos de IA específicos, bem como os requisitos mais relevantes de outras disposições do RGPD, tendo em conta o âmbito do presente parecer.

62. **Princípio da responsabilidade** (artigo 5.º, n.º 2, do RGPD) — Este princípio prevê que o responsável pelo tratamento é responsável pelo cumprimento do RGPD e está em condições de o demonstrar. A este respeito, as funções e responsabilidades das partes que tratam dados pessoais no contexto do desenvolvimento ou da implantação de um modelo de IA devem ser avaliadas antes de o tratamento ter lugar, a fim de definir as obrigações dos responsáveis pelo tratamento ou dos responsáveis conjuntos pelo tratamento, e dos subcontratantes (se existirem), desde o início.

63. **Princípios da licitude, da lealdade e da transparência** (artigo 5.º, n.º 1, alínea a), do RGPD) — Ao avaliar a licitude do tratamento no contexto dos modelos de IA, à luz do artigo 6.º, n.º 1, do RGPD, o CEPD considera útil distinguir as diferentes fases do tratamento de dados pessoais[41]. O princípio da lealdade, que está estreitamente relacionado com o princípio da transparência, exige que os dados pessoais não sejam tratados por métodos desleais, ou por engano, ou de uma forma que seja «*injustificadamente prejudicial, ilegalmente discriminatória, inesperada ou enganadora para o titular dos dados*»[42]. Tendo em conta a complexidade das tecnologias envolvidas, as informações sobre o tratamento de dados pessoais no âmbito dos modelos de IA devem, por conseguinte, ser fornecidas de forma acessível, compreensível e fácil de utilizar[43]. A transparência sobre o tratamento de dados pessoais inclui, em especial, o cumprimento das obrigações de informação previstas nos artigos 12.º a 14.º do RGPD[44], que também exigem, em caso de tomada de decisões automatizada, incluindo a definição de perfis, informações úteis sobre a lógica envolvida, bem como a importância e as consequências previstas do tratamento para o titular dos dados[45]. Tendo em conta que as fases de desenvolvimento dos modelos de IA podem implicar a recolha de grandes quantidades de dados de fontes acessíveis ao público (por exemplo, através de técnicas de raspagem da Web), o recurso à exceção prevista no artigo 14.º, n.º 5, alínea b), do RGPD está estritamente limitado aos casos em que os requisitos desta disposição são plenamente cumpridos[46].

64. **Princípios da limitação da finalidade e da minimização dos dados** (artigo 5.º, n.º 1, alíneas b) e c), do RGPD) - De acordo com o princípio da minimização dos dados, o desenvolvimento e a implantação de modelos de IA exigem que os dados pessoais sejam adequados, pertinentes e necessários em relação à finalidade. Tal pode incluir o tratamento de dados pessoais para evitar os riscos de potenciais enviesamentos e erros quando tal for identificado de forma clara e específica no âmbito da finalidade,

---

[41] Relatório do CEPD sobre o trabalho realizado pelo grupo de trabalho ChatGPT, adotado em 23 de maio de 2024, ponto 14.

[42] Relatório do CEPD sobre o trabalho realizado pelo grupo de trabalho ChatGPT, adotado em 23 de maio de 2024, n.º 23; Orientações 4/2019 do CEPD sobre o artigo 25.º relativo à proteção de dados desde a conceção e por defeito, versão 2.0, adotadas em 20 de outubro de 2020, n.º 69; Orientações do Grupo de Trabalho do artigo 29.º sobre a transparência nos termos do Regulamento 2016/679, revistas e adotadas em 11 de abril de 2018, aprovadas pelo CEPD em 25 de maio de 2018, n.º 2.

[43] Orientações do Grupo de Trabalho do Artigo 29.º sobre a transparência ao abrigo do Regulamento 2016/679, revistas e adoptadas em 11 de abril de 2018, aprovadas pelo CEPD em 25 de maio de 2018, n.º 5.

[44] Ver também o considerando 39 do RGPD que estabelece que «*deve ser transparente para as pessoas singulares que os dados pessoais que lhes digam respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados.[...]*».

[45] Artigo 13.º, n.º 2, alínea f), do RGPD e artigo 14.º, n.º 2, alínea g), do RGPD.

[46] Relatório do CEPD sobre o trabalho realizado pelo grupo de trabalho ChatGPT, adotado em 23 de maio de 2024, ponto 27.

e os dados pessoais forem necessários para essa finalidade (por exemplo, não podem ser eficazmente alcançados através do tratamento de outros dados, incluindo dados sintéticos ou anonimizados)[47]. O GT 29 já salientou que o «*objetivo da recolha deve ser identificado de forma clara e específica* [...]»[48]. Ao avaliar se a finalidade prosseguida é legítima, específica e explícita e se o tratamento cumpre o princípio da minimização dos dados, há que identificar, em primeiro lugar, a atividade de tratamento em causa. Nomeadamente, as diferentes etapas das fases de desenvolvimento ou de implantação podem constituir as mesmas atividades de tratamento ou atividades diferentes, e podem implicar sucessivos responsáveis pelo tratamento ou responsáveis conjuntos pelo tratamento. Em alguns casos, é possível determinar a finalidade que será prosseguida durante a implantação do modelo de IA numa fase de desenvolvimento inicial. Mesmo que não seja esse o caso, o contexto dessa implantação já deve ser claro e, por conseguinte, deve ser considerada a forma como esse contexto informa o objetivo do desenvolvimento. Ao rever a finalidade do tratamento numa determinada fase de desenvolvimento, as AC devem esperar um certo grau de pormenor do(s) responsável(is) pelo tratamento e uma explicação da forma como estes dados informam a finalidade do tratamento. Isto pode incluir, por exemplo, informações sobre o tipo de modelo de IA desenvolvido, as suas funcionalidades esperadas e qualquer outro contexto relevante que já seja conhecido nessa fase. O contexto da utilização pode também incluir, por exemplo, se um modelo está a ser desenvolvido para utilização interna, se o responsável pelo tratamento pretende vender ou distribuir o modelo a terceiros após o seu desenvolvimento, incluindo se o modelo se destina principalmente a ser utilizado para fins de investigação ou comerciais.

65. **Direitos dos titulares dos dados** (capítulo III do RGPD) — Não obstante a necessidade de as autoridades de controlo assegurarem que todos os direitos dos titulares dos dados são respeitados quando os modelos de IA são desenvolvidos e aplicados pelos responsáveis pelo tratamento, o CEPD recorda que, sempre que um responsável pelo tratamento invoque um interesse legítimo como base jurídica, o direito de oposição nos termos do artigo 21.º do RGPD é aplicável e deve ser[49]assegurado.

3.3.2 Considerações sobre as três etapas da avaliação do interesse legítimo no contexto do desenvolvimento e da implantação de modelos de IA

66. Para determinar se um determinado tratamento de dados pessoais pode ser baseado no artigo 6.º, n.º 1, alínea f), do RGPD, as AC devem verificar se os responsáveis pelo tratamento avaliaram cuidadosamente e documentaram se as três condições cumulativas seguintes estão preenchidas: i) a prossecução de um interesse legítimo por parte do responsável pelo tratamento ou de um terceiro; ii)

[47]Além disso, o artigo 10.º, n.º 5, do Regulamento AI prevê regras específicas para o tratamento de categorias especiais de dados pessoais em relação aos sistemas de IA de risco elevado, a fim de assegurar a deteção e a correção de enviesamentos.

[48] Parecer 03/2013 do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades (WP203), páginas 15-16.

[49] Nos termos do artigo 21.º do RGPD, se um titular dos dados se opuser, por motivos relacionados com a sua situação particular, ao tratamento de dados pessoais que lhe digam respeito, o responsável pelo tratamento deixará de tratar os dados pessoais, a menos que o responsável pelo tratamento apresente razões imperiosas e legítimas para o tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados ou para a declaração, o exercício ou a defesa de um direito num processo judicial. Por conseguinte, os dois aspetos a ter em conta pelas AC são se o responsável pelo tratamento está em condições de demonstrar tais razões imperiosas e legítimas e se o direito de oposição pode ser exercido.

o tratamento é necessário para prosseguir o interesse legítimo; e iii) o interesse legítimo não é prevalecer pelos interesses ou direitos e liberdades fundamentais dos titulares dos dados[50].

3.3.2.1 Primeira etapa - Prossecução de um interesse legítimo pelo responsável pelo tratamento ou por um terceiro

67. Um interesse é o interesse ou benefício mais amplo que um responsável pelo tratamento ou um terceiro pode ter no exercício de uma atividade de tratamento específica[51]. Embora o RGPD e o TJUE tenham reconhecido vários interesses como legítimos [52] , a avaliação da legitimidade de um determinado interesse deve ser o resultado de uma análise caso a caso.

68. Tal como recordado pelo CEPD nas suas Orientações sobre interesses legítimos[53], um interesse pode ser considerado legítimo se estiverem preenchidos os três critérios cumulativos seguintes:

    a. O interesse é legítimo[54];

    b. O interesse é articulado de forma clara e precisa; e

    c. O interesse é real e presente, não especulativo.

69. Sob reserva das duas outras etapas exigidas pela avaliação do interesse legítimo, os seguintes exemplos podem constituir um interesse legítimo no contexto dos modelos de IA: i) desenvolvimento do serviço de um agente de conversação para ajudar os utilizadores; ii) desenvolvimento de um sistema de IA para detetar conteúdos ou comportamentos fraudulentos; e iii) melhoria da deteção de ameaças num sistema de informação.

3.3.2.2 Segunda etapa - Análise da necessidade do tratamento para prosseguir o interesse legítimo

70. A segunda etapa da avaliação consiste em determinar se o tratamento de dados pessoais é necessário para a prossecução do(s) interesse(s) legítimo(s) prosseguido(s)[55] ("teste de necessidade").

---

[50] TJUE, acórdão de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 106; TJUE, acórdão de 11 de dezembro de 2019, processo C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), n.º 40. Ver também as Orientações 1/2024 do CEPD sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotadas em 8 de outubro de 2024, n.º 12 e seguintes. Tal como recordado nas presentes orientações, esta «*avaliação deve ser efetuada no início do tratamento, com a participação do responsável pela proteção de dados (RPD) (se designado), e deve ser documentada pelo responsável pelo tratamento em conformidade com o princípio da responsabilização estabelecido no artigo 5.º, n.º 2, do RGPD*».

[51] Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adoptada em 8 de outubro de 2024, ponto 14.

[52] Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 16.

[53] Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 17.

[54] TJUE, acórdão de 4 de outubro de 2024, Processo C-621/22*, Koninklijke Nederlandse Lawn* Tennisbond (ECLI:EU:C:2024:857), ponto 49, em que o TJUE salientou que um interesse legítimo não pode ser contrário à lei. A este respeito, o CEPD salienta que, consoante o caso, os quadros legislativos devem ser tidos em conta na avaliação da legalidade de um determinado interesse. Ver, por exemplo: Artigo 26.º, n.º 3, e artigo 28.º do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) («RSD») sobre a publicidade direcionada proibida a menores; artigo 5.º, n.^{os} 1 e 2, do Regulamento IA sobre práticas de IA proibidas (práticas manipuladoras e abaixo do limiar de consciência); tratamento em violação dos direitos de propriedade intelectual e do disposto na Diretiva (UE) 2019/790 relativa aos direitos de autor e direitos conexos no mercado único digital.

[55] Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, pontos 28-30.

71. O considerando 39 do RGPD precisa que «*os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser razoavelmente alcançada por outros meios»*. De acordo com as orientações anteriores do TJUE e do CEPD, a condição relativa à necessidade do tratamento deve ser analisada à luz dos direitos e liberdades fundamentais dos titulares dos dados e em conjugação com o princípio da minimização dos dados consagrado no artigo 5.º, n.º 1, alínea c),[56]do RGPD.

72. A metodologia referida pelo TJUE tem em conta o contexto do tratamento, bem como os efeitos sobre o responsável pelo tratamento e sobre os titulares dos dados. A avaliação da necessidade implica, por conseguinte, dois elementos: i) se a atividade de tratamento permitirá a prossecução da finalidade[57]; e ii) se não existe uma forma menos intrusiva de prosseguir esta finalidade[58].

73. Por exemplo, e conforme o caso, o volume pretendido de dados pessoais envolvidos no modelo de IA tem de ser avaliado à luz de alternativas menos intrusivas que possam estar razoavelmente disponíveis para atingir de forma igualmente eficaz o objetivo do interesse legítimo prosseguido. Se a prossecução da finalidade também for possível através de um modelo de IA que não implique o tratamento de dados pessoais, o tratamento de dados pessoais deve ser considerado como não necessário. Isto é particularmente relevante para o desenvolvimento de modelos de IA. Ao avaliar se a condição de necessidade está preenchida, as AC devem prestar especial atenção à quantidade de dados pessoais tratados e se é proporcional à prossecução do interesse legítimo em causa, também à luz do princípio da minimização dos dados.

---

[56] TJUE, acórdão de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 108 e 109, remetendo igualmente para o TJUE, acórdão de 11 de dezembro de 2019, processo C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), n.º 48; TJUE, acórdão de 9 de novembro de 2010, processos apensos C-92/09 e C-93/09, Volker und Markus Schecke (ECLI:EU:C:2010:662), n.ºs 85 e 86; TJUE, acórdão de 22 de junho de 2021, processo C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), n.ºs 98, 109, 110, 113. Ver também, por exemplo: Orientações do CEPD 3/2019 sobre o tratamento de dados pessoais através de dispositivos de vídeo, versão 2.0, adotadas em 29 de janeiro de 2020, pontos 24-26 e 73; Orientações do CEPD 2/2019 sobre o tratamento de dados pessoais nos termos do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha a titulares de dados, versão 2.0, adotadas em 8 de outubro de 2019, pontos 23-25; Parecer do CEPD 11/2024 sobre a utilização do reconhecimento facial para simplificar o fluxo de passageiros nos aeroportos, versão 1.1, adotado em 23 de maio de 2024, ponto 27.

[57] Ver TJUE, acórdão de 16 de dezembro de 2008, Processo C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), n.º 66. Also in the same case, see the Opinion of Advocate General Poiares Maduro in Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), paragraph 16, stating: «*neste caso, o critério adequado é o da efetividade e cabe ao órgão jurisdicional nacional aplicá-lo. A questão que deve colocar é a de saber se existem outras formas de tratamento de dados através das quais as autoridades de imigração poderiam aplicar as regras relativas ao estatuto de residência. Se responder a esta questão de forma afirmativa, o armazenamento e o tratamento centralizados de dados para os cidadãos da União devem ser declarados ilegais. Não é necessário que o sistema alternativo seja o mais eficaz ou adequado; basta que seja capaz de funcionar adequadamente. Por outras palavras, mesmo que o registo central seja mais eficaz, mais cómodo ou mais fácil de utilizar do que as suas alternativas (como os registos locais descentralizados), estes últimos são claramente preferíveis se puderem ser utilizados para indicar o estatuto de residência dos cidadãos da União*.

[58]Ver TJUE, acórdão de 27 de setembro de 2017, Processo C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), ponto 113: *Cabe, portanto, ao órgão jurisdicional nacional verificar se o estabelecimento da lista impugnada e a inclusão dos nomes dos titulares dos dados nesse registo são adequados para alcançar os objetivos por eles prosseguidos e se não existem outros meios menos restritivos para alcançar esses objetivos*.» Ver também, por exemplo, as conclusões do advogado-geral Rantos no processo C-252/21, *Meta contra Bundeskartellamt*, ECLI:EU:C:2022:704, n.º 61, que enuncia: *'[...] Por conseguinte, é necessário que exista uma ligação estreita entre o tratamento e o interesse prosseguido, na ausência de alternativas mais favoráveis à proteção de dados, uma vez que não é suficiente que o tratamento se limite a ser útil para o responsável pelo tratamento»*.

74. A avaliação da necessidade deve também ter em conta o contexto mais alargado do tratamento previsto dos dados pessoais. A existência de meios menos intrusivos para os direitos e liberdades fundamentais dos titulares dos dados pode variar consoante o responsável pelo tratamento tenha ou não uma relação direta com os titulares dos dados (dados de origem) ou não (dados de terceiros). O TJUE apresentou algumas considerações a ter em conta ao analisar a necessidade do tratamento de dados de terceiros para efeitos do(s) interesse(s) legítimo(s) prosseguido(s) (embora no contexto da divulgação desses dados a terceiros)[59].

75. A aplicação de garantias técnicas para proteger os dados pessoais pode também contribuir para satisfazer o critério da necessidade. Tal poderá incluir, por exemplo, medidas de execução, como as identificadas na secção 3.2.2, de forma a que a anonimização não seja alcançada, mas que continue a reduzir a facilidade com que os titulares dos dados podem ser identificados. O CEPD observa que algumas destas medidas, quando não são necessárias para cumprir o RGPD, podem constituir garantias adicionais, tal como analisado mais pormenorizadamente na subsecção «Medidas de atenuação» da secção 3.3.2.3[60].

3.3.2.3 Terceira etapa - Teste de equilíbrio

76. A terceira etapa da avaliação do interesse legítimo é o «**exercício de equilíbrio**» (também referido no presente documento como «**teste de ponderação**»)[61]. Esta etapa consiste em identificar e descrever os diferentes direitos e interesses opostos em jogo[62], ou seja, por um lado, os interesses, os direitos e liberdades fundamentais dos titulares dos dados e, por outro lado, os interesses do responsável pelo tratamento ou de um terceiro. As circunstâncias específicas do caso devem então ser consideradas para demonstrar que o interesse legítimo é uma base jurídica adequada para as atividades de tratamento em causa[63].

Interesses, direitos e liberdades fundamentais dos titulares dos dados

77. O artigo 6.º, n.º 1, alínea f), do RGPD prevê que, ao avaliar os diferentes componentes no contexto do critério da ponderação, o responsável pelo tratamento deve ter em conta os interesses, os direitos e as liberdades fundamentais dos titulares dos dados. Os interesses dos titulares dos dados são aqueles que podem ser afetados pelo tratamento em causa. No contexto da fase de desenvolvimento de um modelo de IA, estes podem incluir, mas não se limitam a, o interesse na autodeterminação e na manutenção do controlo sobre os próprios dados pessoais (por exemplo, os dados recolhidos para o desenvolvimento do modelo). No contexto da implantação de um modelo de IA, os interesses dos titulares dos dados podem incluir, mas não se limitam a, interesses em manter o controlo sobre os seus próprios dados pessoais (por exemplo, os dados tratados quando o modelo é implantado), interesses financeiros (por exemplo quando um modelo de IA é utilizado pelo titular dos dados para gerar receitas ou é utilizado por uma pessoa no contexto da sua atividade profissional), benefícios pessoais (por exemplo, quando um modelo de IA é utilizado para melhorar a acessibilidade a determinados serviços) ou interesses socioeconómicos (por exemplo, quando um modelo de IA

[59] TJUE, acórdão de 4 de outubro de 2024, Processo C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), n.ºs 51-53.
[60] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 57.
[61] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, pontos 31 a 60.
[62] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 32.
[63] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, n.º 32, referindo-se também ao TJUE, acórdão de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), n.º 110.

permite o acesso a melhores cuidados de saúde ou facilita o exercício de um direito fundamental, como o acesso à educação)[64].

78. Quanto mais precisamente um interesse é definido à luz da finalidade prevista do tratamento, melhor permitirá compreender claramente a realidade dos benefícios e riscos a ter em conta na avaliação do equilíbrio.

79. No que diz respeito aos direitos e liberdades fundamentais dos titulares dos dados, o desenvolvimento e a implantação de modelos de IA podem suscitar sérios riscos para os direitos protegidos pela Carta dos Direitos Fundamentais da UE (a «**Carta da UE**»), incluindo, entre outros, o direito à vida privada e familiar (artigo 7.º da Carta da UE) e o direito à proteção dos dados pessoais (artigo 8.º da Carta da UE). Estes riscos podem ocorrer durante a fase de desenvolvimento, por exemplo quando os dados pessoais são suprimidos contra os desejos dos titulares dos dados ou sem o seu conhecimento. Estes riscos podem também ocorrer na fase de implantação, por exemplo, quando os dados pessoais são tratados pelo modelo (ou como parte dele) de uma forma que viola os direitos das pessoas em causa, ou quando é possível inferir, acidentalmente ou através de ataques (por exemplo, inferência de associação, extração ou inversão do modelo), quais os dados pessoais contidos na base de dados de aprendizagem. Estas situações representam um risco para a privacidade dos titulares dos dados cujos dados podem aparecer na fase de implantação do sistema de IA (por exemplo, risco para a reputação, roubo de identidade ou fraude, risco de segurança, dependendo da natureza dos dados).

80. Dependendo do caso em apreço, podem também existir riscos para outros direitos fundamentais. Por exemplo, a recolha de dados em grande escala e indiscriminada por modelos de IA na fase de desenvolvimento pode criar um sentimento de vigilância para os titulares dos dados, especialmente tendo em conta as dificuldades em evitar que os dados públicos sejam raspados. Esta situação pode levar as pessoas a autocensurarem-se e apresenta riscos de comprometer a sua liberdade de expressão (artigo 11.º da Carta da UE). Na fase de implantação, os riscos para a liberdade de expressão também estão presentes quando os modelos de IA são utilizados para bloquear a publicação de conteúdos dos titulares dos dados. Além disso, um modelo de IA que recomende conteúdos inadequados a indivíduos vulneráveis pode representar riscos para a sua saúde mental (artigo 3.º, n.º 1, da Carta da UE). Noutros casos, a implantação de modelos de IA pode também ter consequências adversas para o direito individual de trabalhar (artigo 15.º da Carta da UE), por exemplo, quando as candidaturas a emprego são pré-selecionadas utilizando um modelo de IA. Da mesma forma, um modelo de IA pode apresentar riscos para o direito à não discriminação (artigo 21.º da Carta da UE), se discriminar indivíduos com base em determinadas caraterísticas pessoais (como a nacionalidade ou o género). Além disso, a implantação de modelos de IA pode também apresentar riscos para a segurança e a proteção do indivíduo (por exemplo, quando o modelo de IA é utilizado com intenções maliciosas), bem como riscos para a sua integridade física e mental[65].

81. A implantação de modelos de IA pode também ter um impacto positivo em determinados direitos fundamentais, por exemplo, o modelo pode apoiar o direito à integridade mental da pessoa (artigo 3.º da Carta), por exemplo, quando um modelo de IA é utilizado para identificar conteúdos nocivos em linha; ou o modelo pode facilitar o acesso a determinados serviços essenciais ou facilitar o exercício de direitos fundamentais, como o acesso à informação (artigo 11.º da Carta da UE) ou o acesso à educação (artigo 14.º da Carta da UE).

[64] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 38.
[65] Orientações 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotada em 8 de outubro de 2024, ponto 46.

Impacto do tratamento nos sujeitos dos dadoscts

82. O tratamento de dados pessoais que ocorre durante o desenvolvimento e a implantação de modelos de IA pode afetar os titulares dos dados de diferentes formas, o que pode ser positivo ou negativo[66]. Por exemplo, se uma atividade de tratamento implicar benefícios para o titular dos dados, estes podem ser tidos em conta na avaliação do equilíbrio. Embora a existência de tais benefícios possa levar à conclusão, por parte de uma AC, de que os interesses do responsável pelo tratamento ou de um terceiro não se sobrepõem aos interesses, direitos e liberdades fundamentais dos titulares dos dados, essa conclusão só pode ser o resultado de uma análise caso a caso, tendo em conta todos os fatores adequados.

83. O impacto do tratamento nos titulares dos dados pode ser influenciado (i) pela natureza dos dados tratados pelos modelos; (ii) pelo contexto do tratamento; e (iii) pelas consequências adicionais que o tratamento pode ter[67].

84. Em relação à **natureza dos dados tratados**, importa recordar que — para além das categorias especiais de dados pessoais e de dados relativos a condenações e infrações penais que, respetivamente, beneficiam de proteção adicional nos termos dos artigos 9.º e 10.º do RGPD — o tratamento de algumas outras categorias de dados pessoais pode ter consequências significativas para os titulares dos dados. Neste contexto, o tratamento de certos tipos de dados pessoais que revelam informações altamente privadas (por exemplo, dados financeiros ou dados de localização) para o desenvolvimento e a implantação de um modelo de IA deve ser considerado como podendo ter um impacto grave nas pessoas em causa. Na fase de implantação, as consequências desse tratamento para os titulares dos dados podem, por exemplo, ser económicas (por exemplo, discriminação no contexto do emprego) e/ou reputacionais (por exemplo, difamação).

85. Em relação ao **contexto do tratamento,** é necessário, em primeiro lugar, identificar os elementos que podem criar riscos para os titulares dos dados (por exemplo, a forma como o modelo foi desenvolvido, a forma como o modelo pode ser utilizado e/ou se as medidas de segurança utilizadas para proteger os dados pessoais são adequadas). A natureza do modelo e as utilizações operacionais previstas desempenham um papel fundamental na identificação dessas causas potenciais.

86. É igualmente necessário avaliar a gravidade destes riscos para os titulares dos dados. Pode considerar-se, entre outras coisas, a forma como os dados pessoais são tratados (por exemplo, se forem combinados com outros conjuntos de dados), qual é a escala do tratamento e a quantidade de dados pessoais tratados[68] (por exemplo, o volume global de dados, o volume de dados por titular dos dados, o número de titulares de dados afetados),[69]o estatuto do titular dos dados (por exemplo, crianças ou outros titulares de dados vulneráveis) e a sua relação com o responsável pelo tratamento (por exemplo, se o titular dos dados for um cliente). Por exemplo, a utilização da recolha de material na Web na fase de desenvolvimento pode conduzir — na ausência de garantias suficientes — a impactos significativos nas pessoas, devido ao grande volume de dados recolhidos, ao elevado número de titulares de dados e à recolha indiscriminada de dados pessoais.

[66] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 39.
[67] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 32.
[68] Ver Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 43.
[69] TJUE, acórdão de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), parágrafo 116.

87. As **outras consequências** que o tratamento pode ter também devem ser tidas em conta na avaliação do impacto do tratamento nos titulares dos dados. Devem ser avaliadas pelas AC caso a caso, tendo em conta os factos específicos em causa.

88. Tais consequências podem incluir (mas não se limitam a) riscos de violação dos direitos fundamentais dos titulares dos dados, tal como descrito na subsecção anterior[70]. Os riscos podem variar em termos de probabilidade e gravidade e podem resultar do tratamento de dados pessoais que possa conduzir a danos físicos, materiais ou não materiais, em especial quando o tratamento possa dar origem a discriminação[71].

89. Sempre que a implantação de um modelo de IA implique o tratamento de dados pessoais de (i) titulares de dados cujos dados pessoais estejam incluídos no conjunto de dados utilizado na fase de desenvolvimento; e (ii) titulares de dados cujos dados pessoais sejam tratados na fase de implantação, as AC devem distinguir e ter em conta os riscos que afetam os interesses, os direitos e as liberdades de cada uma destas categorias de titulares de dados aquando da verificação do teste de equilíbrio realizado por um responsável pelo tratamento.

90. **Por último, a análise das possíveis consequências posteriores do tratamento deve também considerar a probabilidade de essas consequências posteriores se concretizarem**. A avaliação dessa probabilidade deve ser efetuada tendo em conta as medidas técnicas e organizacionais em vigor e as circunstâncias específicas do caso. Por exemplo, as AC podem considerar se foram aplicadas medidas para evitar uma potencial utilização abusiva do modelo de IA. Para os modelos de IA que podem ser implantados para uma variedade de fins, como a IA generativa, tal pode incluir controlos que limitem tanto quanto possível a sua utilização para práticas nocivas, por exemplo: a criação de deepfakes; chatbots que são utilizados para desinformação, phishing e outros tipos de fraude; e agentes manipuladores de IA/AI (em particular quando são antropomórficos ou fornecem informações enganosas).

Expectativas razoáveis dos titulares dos dados

91. Com base no considerando 47 do RGPD, *«[a]tualmente, a existência de um interesse legítimo requer uma avaliação cuidadosa, incluindo a questão de saber se a pessoa em causa pode razoavelmente esperar, no momento e no contexto da recolha dos dados pessoais, que o tratamento para essa finalidade possa ter lugar.* [72]*Os interesses e os direitos fundamentais do titular dos dados podem, em especial, sobrepor-se aos interesses do responsável pelo tratamento quando os dados pessoais são tratados em circunstâncias em que os titulares dos dados não esperam razoavelmente um tratamento posterior»*.

92. As expectativas razoáveis desempenham um papel fundamental no critério de equilíbrio, nomeadamente devido à complexidade da tecnologia utilizada nos modelos de IA e ao facto de poder ser difícil para os titulares dos dados compreender a variedade de utilizações potenciais de um modelo

[70]Ver a subsecção «Interesses, direitos e liberdades fundamentais dos titulares dos dados» supra.

[71] Ver Secção 2.3 das Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024. Ver também o considerando 75 do RGPD para mais exemplos.

[72] Ver também TJUE, acórdão de 4 de julho de 2023, processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), n.º 112; TJUE, acórdão de 11 de dezembro de 2019, processo C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), n.º 58; TJUE, acórdão de 4 de outubro de 2024, processo C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), n.º 55.

de IA e o tratamento de dados envolvido[73]. Para o efeito, a informação fornecida às pessoas em causa pode ser considerada para avaliar se as pessoas em causa podem razoavelmente esperar que os seus dados pessoais sejam tratados. No entanto, embora a omissão de informações possa contribuir para que os titulares dos dados não esperem um determinado tratamento, o simples cumprimento dos requisitos de transparência estabelecidos no RGPD não é, por si só, suficiente para considerar que os titulares dos dados podem razoavelmente esperar um determinado tratamento[74]. Além disso, o simples facto de a informação relacionada com a fase de desenvolvimento de um modelo de IA estar incluída na política de privacidade do responsável pelo tratamento não significa necessariamente que as pessoas em causa possam razoavelmente esperar que isso aconteça; pelo contrário, isto deve ser analisado pelas SCV com base nas circunstâncias específicas do caso e considerando todos os factores relevantes.

93. Ao avaliar as expetativas razoáveis dos titulares dos dados em relação ao tratamento que ocorre na fase de desenvolvimento, é importante referir os elementos mencionados nas Diretrizes do CEPD sobre o interesse legítimo[75]. Além disso, no âmbito do objeto do presente parecer, é importante ter em conta o contexto mais amplo do tratamento. Tal pode incluir, embora não exclusivamente, se os dados pessoais estavam ou não disponíveis ao público, a natureza da relação entre o titular dos dados e o responsável pelo tratamento (e se existe ou não uma ligação entre os dois), a natureza do serviço, o contexto em que os dados pessoais foram recolhidos, a fonte a partir da qual os dados foram recolhidos (por exemplo, o sítio Web ou o serviço onde os dados pessoais foram recolhidos e as definições de privacidade que oferecem), as potenciais utilizações adicionais do modelo e se os titulares dos dados estão efetivamente cientes de que os seus dados pessoais estão ou não em linha.

94. Na fase de desenvolvimento do modelo, as expetativas razoáveis dos titulares dos dados podem diferir consoante os dados tratados para desenvolver o modelo sejam ou não tornados públicos pelos titulares dos dados. Além disso, as expetativas razoáveis podem também variar em função do facto de terem fornecido diretamente os dados ao responsável pelo tratamento (por exemplo, no contexto da sua utilização do serviço) ou de o responsável pelo tratamento os ter obtido de outra fonte (por exemplo, através de um terceiro, ou raspagem). Em ambos os casos, as medidas tomadas para informar os titulares dos dados sobre as atividades de tratamento devem ser tidas em conta na avaliação das expetativas razoáveis.

95. Na fase de implantação do modelo de IA, é igualmente importante ter em conta as expetativas razoáveis dos titulares dos dados no contexto das capacidades específicas do modelo. Por exemplo, no caso de modelos de IA que podem adaptar-se de acordo com os dados fornecidos, pode ser relevante considerar se as pessoas em causa estavam cientes de que tinham fornecido dados pessoais para que o modelo de IA pudesse ajustar as suas respostas às suas necessidades e para que pudessem obter serviços personalizados. Além disso, pode também ser relevante considerar se esta atividade de tratamento só teria impacto no serviço prestado aos titulares dos dados (por exemplo, a

[73] Por exemplo, no acórdão de 4 de julho de 2023, Processo C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), parágrafo 123, embora o TJUE tenha considerado que a «melhoria do produto» não pode, em princípio, ser excluída como um interesse legítimo, considerou também que é «*duvidoso que [...] o objetivo de «melhorar o produto», tendo em conta a escala desse tratamento e o seu impacto significativo no utilizador, bem como o facto de o utilizador não poder razoavelmente esperar que esses dados sejam tratados [...] pode sobrepor-se aos interesses e direitos fundamentais desse utilizador, particularmente no caso de esse utilizador ser uma criança*».

[74]Orientações 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotadas em 8 de outubro de 2024, ponto 53.

[75] Orientações 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotadas em 8 de outubro de 2024, parágrafos 50 a 54.

personalização do conteúdo para um utilizador específico) ou se seria utilizada para modificar o serviço prestado a todos os clientes (por exemplo, para melhorar o modelo de uma forma geral). Tal como na fase de desenvolvimento, pode também ser particularmente relevante considerar se existe uma ligação direta entre os titulares dos dados e o responsável pelo tratamento. Tal ligação direta pode, por exemplo, permitir que o responsável pelo tratamento forneça facilmente informações aos titulares dos dados sobre a atividade de tratamento e o modelo, o que poderia influenciar as expetativas razoáveis desses titulares dos dados.

Medidas de atenuação

96. Quando os interesses, direitos e liberdades das pessoas em causa parecerem sobrepor-se ao(s) interesse(s) legítimo(s) prosseguido(s) pelo responsável pelo tratamento ou por um terceiro, o responsável pelo tratamento pode considerar a introdução de medidas atenuantes para limitar o impacto do tratamento sobre essas pessoas. As medidas atenuantes são salvaguardas que devem ser adaptadas às circunstâncias do caso e dependem de diferentes factores, incluindo a utilização prevista do modelo de IA. Estas medidas de atenuação destinam-se a assegurar que os interesses do responsável pelo tratamento ou de terceiros não sejam derrogados, de modo a que o responsável pelo tratamento possa invocar esta base jurídica.

97. Como recordado nas Orientações do CEPD sobre o interesse legítimo, as medidas atenuantes não devem ser confundidas com as medidas que o responsável pelo tratamento é legalmente obrigado a adotar de qualquer forma para garantir a conformidade com o RGPD, independentemente de o tratamento se basear no artigo 6.º, n.º 1, alínea f), do RGPD[76]. Isto é particularmente importante para as medidas que, por exemplo, exigem o cumprimento dos princípios do RGPD, como o princípio da minimização dos dados.

98. A lista de medidas apresentada abaixo não é exaustiva e não prescritiva e a aplicação das medidas deve ser considerada numa avaliação caso a caso. Embora, dependendo das circunstâncias, algumas das medidas abaixo possam ser necessárias para cumprir obrigações específicas do RGPD, quando não for esse o caso, podem ser tidas em conta como salvaguardas adicionais. Além disso, algumas das medidas a seguir mencionadas dizem respeito a domínios que estão sujeitos a uma rápida evolução e a novos desenvolvimentos e devem ser tidas em conta pelas AC no tratamento de um caso específico.

99. **Em relação à fase de desenvolvimento dos modelos de IA**, podem ser tomadas várias medidas para atenuar os riscos colocados pelo tratamento de dados próprios e de terceiros (incluindo para atenuar os riscos relacionados com as práticas de recolha de dados na Web). Com base no que precede, o CEPD apresenta alguns exemplos de medidas que podem ser aplicadas para atenuar os riscos identificados no critério do equilíbrio e que devem ser tidas em conta pelas AC na avaliação de modelos de IA específicos caso a caso.

100. **Medidas técnicas**

    a. Medidas mencionadas na Secção 3.2.2 que sejam adequadas para atenuar os riscos em jogo, quando essas medidas não resultem na anonimização do modelo e não sejam necessárias para cumprir outras obrigações do RGPD ou ao abrigo do teste de necessidade (segunda etapa da avaliação do interesse legítimo).

101. Para além destas, outras medidas pertinentes podem incluir:

[76]Orientações 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotadas em 8 de outubro de 2024, ponto 57.

b. Medidas de pseudonimização: tal poderá incluir, por exemplo, medidas para evitar qualquer combinação de dados com base em identificadores individuais. Estas medidas podem não ser adequadas se a AC considerar que o responsável pelo tratamento demonstrou a necessidade razoável de recolher dados diferentes sobre uma determinada pessoa para o desenvolvimento do sistema ou modelo de IA em questão.

c. Medidas para ocultar dados pessoais ou substituí-los por dados pessoais falsos no conjunto de formação (por exemplo, a substituição de nomes e endereços de correio eletrónico por nomes falsos e endereços de correio eletrónico falsos). Esta medida pode ser particularmente adequada quando o conteúdo substantivo real dos dados não é relevante para o tratamento global (por exemplo, em ações de formação ao longo da vida).

102. **Medidas que facilitem o exercício dos direitos individuais:**

a. Observar um período de tempo razoável entre a recolha de um conjunto de dados de formação e a sua utilização. Esta salvaguarda adicional pode permitir que as pessoas em causa exerçam os seus direitos durante este período, sendo o período de tempo razoável avaliado em função das circunstâncias de cada caso.

b. Propor, desde o início, uma «opt-out» incondicional, prevendo, por exemplo, um direito discricionário de oposição aos titulares dos dados antes de o tratamento ter lugar, a fim de reforçar o controlo das pessoas sobre os seus dados, o que vai além das condições previstas no artigo 21.º do RGPD[77].

c. Permitir que os titulares dos dados exerçam o seu direito de apagamento mesmo quando os motivos específicos enumerados no artigo 17.º, n.º 1, do RGPD não são aplicáveis[78].

d. Permitir que as pessoas em causa apresentem alegações de regurgitação ou memorização de dados pessoais e as circunstâncias e meios pelos quais as alegações podem ser reproduzidas, permitindo que os responsáveis pelo tratamento reproduzam e avaliem as técnicas de desaprendizagem pertinentes para dar resposta às alegações.

103. **Medidas de transparência:** em alguns casos, as medidas de atenuação podem incluir medidas que proporcionem maior transparência no que diz respeito ao desenvolvimento do modelo de IA. Algumas medidas, para além do cumprimento das obrigações do RGPD, podem ajudar a superar a assimetria da informação e permitir que os titulares dos dados obtenham uma melhor compreensão do tratamento envolvido na fase de desenvolvimento:

a. Publicação de comunicações públicas e facilmente acessíveis que vão além das informações exigidas nos termos dos artigos 13.º ou 14.º do RGPD, por exemplo, fornecendo pormenores adicionais sobre os critérios de recolha e todos os conjuntos de dados utilizados, tendo em conta a proteção especial das crianças e das pessoas vulneráveis.

b. Formas alternativas de informar as pessoas em causa, por exemplo: campanhas mediáticas com diferentes meios de comunicação social para informar as pessoas em causa, campanha de informação por correio eletrónico, utilização de visualização gráfica, perguntas frequentes, rótulos de transparência e fichas-modelo, cuja sistematização poderia estruturar a apresentação de informações sobre modelos de IA, e relatórios anuais de transparência numa base voluntária.

[77] Ibid.
[78] Ibid.

104. **<u>Medidas de atenuação específicas no contexto da raspagem da Web</u>:** Tendo em conta que, tal como acima referido, a raspagem na Web aumenta riscos específicos[79], poderiam ser identificadas medidas de atenuação específicas neste contexto. Se for caso disso, podem ser consideradas pelas AC, para além das medidas de atenuação acima mencionadas, ao investigarem os responsáveis pelo tratamento de dados que efetuam a raspagem da Web.

105. Medidas específicas, quando não necessárias na segunda etapa da avaliação do interesse legítimo, podem revelar-se úteis para atenuar o risco no contexto da raspagem da Web. Estas podem incluir **medidas técnicas**, tais como:

    a. A exclusão de conteúdos de dados de publicações que possam incluir dados pessoais que impliquem riscos para determinadas pessoas ou grupos de pessoas (por exemplo, pessoas que possam ser objeto de abuso, prejuízo ou mesmo danos físicos se as informações forem divulgadas publicamente).

    b. Assegurar que determinadas categorias de dados não são recolhidas ou que determinadas fontes são excluídas da recolha de dados, o que pode incluir, por exemplo, determinados sítios Web que são particularmente intrusivos devido à sensibilidade do seu objeto.

    c. Excluir a recolha de sítios Web (ou secções de sítios Web) que se oponham claramente à raspagem da Web e à reutilização dos seus conteúdos para efeitos de criação de bases de dados de formação em IA (por exemplo, respeitando os ficheiros robots.txt ou ai.txt ou qualquer outro mecanismo reconhecido para expressar a exclusão da recolha automática ou raspagem).

    d. Imposição de outros limites relevantes à recolha, incluindo eventualmente critérios baseados em períodos de tempo.

106. No contexto da raspagem na Web, os exemplos de medidas específicas **que facilitam o exercício dos direitos e da transparência das pessoas** podem incluir: a criação de uma lista de autoexclusão, gerida pelo responsável pelo tratamento e que permite que os titulares dos dados se oponham à recolha dos seus dados em determinados sítios Web ou plataformas em linha, fornecendo informações que os identifiquem nesses sítios Web, nomeadamente antes de a recolha de dados ocorrer[80].

107. **<u>Considerações específicas relativas às medidas de atenuação na fase de implantação</u>:** Embora algumas das medidas acima mencionadas possam também ser relevantes para a fase de implantação, em função das circunstâncias, o CEPD apresenta abaixo uma lista não exaustiva de medidas de apoio adicionais que podem ser aplicadas e que devem ser avaliadas pelas autoridades de controlo caso a caso.

    a. Podem, por exemplo, ser adotadas **medidas técnicas** para evitar o armazenamento, a regurgitação ou a geração de dados pessoais, especialmente no contexto de modelos de IA generativos (tais como filtros de saída) e/ou para atenuar o risco de reutilização ilegal por

[79] Estas práticas podem também levantar outras questões que não são abrangidas pelo presente parecer, ver, por exemplo, Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law.* European Journal of Privacy Law & Technologies, (2023) 2 p. 1 - 19, disponível em: https://doi.org/10.57230/EJPLT232PS.

[80] A menos que o responsável pelo tratamento demonstre a existência de razões imperiosas e legítimas para o tratamento que prevaleçam sobre os interesses, direitos e liberdades da pessoa em causa ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

modelos de IA de finalidade geral (por exemplo, marcação digital de água dos resultados gerados pela IA).

b. **Medidas que facilitem ou acelerem o exercício dos direitos das pessoas singulares** na fase de implementação, para além do que é exigido por lei, nomeadamente no que diz respeito ao exercício do direito ao apagamento de dados pessoais a partir de dados de saída de modelos ou à desduplicação, e às técnicas pós-formação que tentam eliminar ou suprimir dados pessoais.

108. Ao investigar a implantação de um modelo de IA específico, as AC devem considerar se o responsável pelo tratamento publicou o teste de equilíbrio que efetuou, uma vez que isso pode aumentar a transparência e a equidade. Tal como mencionado nas Orientações do CEPD sobre interesse legítimo, podem ser consideradas outras medidas para fornecer aos titulares dos dados informações sobre o teste de equilíbrio antes de qualquer recolha de dados pessoais[81]. O CEPD reitera igualmente[82] que um elemento a considerar é se o responsável pelo tratamento envolveu ou não o encarregado da proteção de dados, quando aplicável.

3.4 Sobre o possível impacto de um tratamento ilegal no desenvolvimento de um modelo de IA sobre a legalidade do tratamento ou funcionamento subsequente do modelo de IA

109. A presente secção do parecer aborda a pergunta 4 do pedido. Esta pergunta procura clarificar o possível impacto de um tratamento ilegal na fase de desenvolvimento sobre o tratamento subsequente (por exemplo, na fase de implantação do modelo de IA) ou sobre o funcionamento do modelo. A pergunta visa abordar tanto a situação em que esse modelo de IA trata dados pessoais que são conservados no modelo (pergunta 4, alínea i), do pedido) como a situação em que já não existe tratamento de dados pessoais envolvido na aplicação do modelo de IA (ou seja, o modelo é anónimo) (pergunta 4, alínea ii), do pedido).

110. Antes de abordar determinados cenários específicos, o CEPD apresenta as seguintes considerações gerais.

111. Em primeiro lugar, os esclarecimentos prestados na presente secção centrar-se-ão no tratamento de dados pessoais na fase de desenvolvimento realizada sem respeitar o princípio da licitude, tal como estabelecido especificamente no artigo 5.º, n.º 1, alínea a), e no artigo 6.º do RGPD (a seguir designada «**ilegalidade**»)[83]. Do mesmo modo, as considerações do CEPD centrar-se-ão no impacto da ilegalidade do tratamento na fase de desenvolvimento sobre a licitude (ou seja, a conformidade com o artigo 5.º, n.º 1, alínea a), do RGPD e com o artigo 6.º do RGPD) do tratamento ou funcionamento subsequente do modelo. No entanto, o CEPD salienta que o tratamento efetuado na fase de desenvolvimento pode também conduzir a violações de outras disposições do RGPD, como a falta de transparência para com os titulares dos dados ou a proteção de dados desde a conceção e/ou por defeito, que não são analisadas no presente parecer.

[81] Orientações CEPD 1/2024 sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, Versão 1.0, adotada em 8 de outubro de 2024, ponto 68.
Orientações 1/2024 do[82] CEPD sobre o tratamento de dados pessoais com base no artigo 6.º, n.º 1, alínea f), do RGPD, versão 1.0, adotada em 8 de outubro de 2024, ponto 12.
[83]TJUE, acórdão de 4 de maio de 2023, Processo C-60/22*, Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), pontos 55-57.

112. Em segundo lugar, ao abordar esta questão, o princípio da responsabilidade, que exige que os responsáveis pelo tratamento sejam responsáveis pelo cumprimento, e demonstrem o cumprimento, *nomeadamente*, do artigo 5.º, n.º 1, do RGPD e do artigo 6.º do RGPD[84], desempenha um papel fundamental. O mesmo se aplica à necessidade de avaliar qual a organização que é responsável pelo tratamento para a atividade de tratamento em causa e se surgem situações de responsabilidade conjunta pelo tratamento (uma vez que podem estar indissociavelmente ligadas)[85]. Tendo em conta a importância das circunstâncias factuais de cada caso, nomeadamente no que diz respeito ao papel desempenhado por cada parte envolvida no tratamento, as considerações do CEPD devem ser entendidas como observações gerais que devem ser avaliadas caso a caso pelas autoridades de controlo.

113. Em terceiro lugar, o CEPD salienta que, em conformidade com o artigo 51.º, n.º 1, do RGPD, as autoridades de controlo são «*responsáveis pelo controlo da aplicação do [RGPD], a fim de proteger os direitos e liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento e facilitar a livre circulação de dados pessoais na União*». Por conseguinte, é da competência das autoridades de controlo avaliar a licitude do tratamento e exercer os poderes que lhes são conferidos pelo RGPD em conformidade com o seu quadro nacional[86]. Nesses casos, as AC dispõem de poderes discricionários para avaliar a(s) possível(is) infração(ões) e escolher as medidas adequadas, necessárias e proporcionadas, entre as mencionadas no artigo 58.º do RGPD, tendo em conta as circunstâncias de cada caso individual[87].

114. **Quando se constata uma infração, as AC podem impor medidas corretivas, como ordenar aos responsáveis pelo tratamento, tendo em conta as circunstâncias de cada caso, que tomem medidas para remediar a ilegalidade do tratamento inicial.** Estes podem incluir, por exemplo, a emissão de uma coima, a imposição de uma limitação temporária ao tratamento, o apagamento de parte do conjunto de dados que foi tratado ilegalmente ou, se tal não for possível, dependendo dos factos em causa, tendo em conta a proporcionalidade da medida, ordenar o apagamento de todo o conjunto de dados utilizado para desenvolver o modelo de IA e/ou o próprio modelo de IA. Ao avaliar a proporcionalidade da medida prevista, as AC podem ter em conta as medidas que podem ser aplicadas pelo responsável pelo tratamento para remediar a ilegalidade do tratamento inicial (por exemplo, reciclagem profissional).

[84]TJUE, acórdão de 4 de maio de 2023, Processo C-60/22*, Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), ponto 53.

[85] Orientações 07/2020 do CEPD sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD, versão 2.1, adotadas em 7 de julho de 2021, pont0 55.

[86] Poderá ser necessário ter em conta regras nacionais específicas. Ver, por exemplo, o artigo 2.º-decisões do Código de Proteção de Dados italiano (Decreto legislativo n.º 196/2003), que estabelece que os dados tratados em violação das regras de proteção de dados não podem ser utilizados. Isto sem prejuízo de outros quadros jurídicos nacionais, como o direito penal.

[87]Ver, a este respeito, o considerando 129 do RGPD, bem como o acórdão do TJUE de 26 de setembro de 2024, processo C-768-21, T R/*Land Hessen* (ECLI:EU:C:2024:785), ponto 37; acórdão do TJUE de 7 de dezembro de 2023, nos processos apensos C-26/22 e C-64/22, SCHUFA Holding (Libération de reliquat det dette) (ECLI:EU:C:2023:958), ponto 57; e TJUE, acórdão de 14 de março de 2024, Processo C-46/23, Újpesti Polgármesteri Hivatal *(* ECLI:EU:C:2024:239), ponto 34.

115. O CEPD salienta ainda que, quando os dados pessoais são tratados ilegalmente, os titulares dos dados podem solicitar o apagamento dos seus dados pessoais, nas condições previstas no artigo 17.º do RGPD, e que as AC podem ordenar o apagamento dos dados pessoais *ex officio*[88].

116. Ao avaliar se uma medida é adequada, necessária e proporcionada, as autoridades de controlo podem ter em conta, entre outros elementos, os riscos suscitados para os titulares dos dados, a gravidade da infração, a viabilidade técnica e financeira da medida, bem como o volume de dados pessoais envolvidos.

117. Por último, o CEPD recorda que as medidas tomadas pelas AC ao abrigo do RGPD não prejudicam as medidas tomadas pelas autoridades competentes ao abrigo da Lei da IA e/ou de outros quadros jurídicos aplicáveis (por exemplo, legislação sobre responsabilidade civil).

118. Nas secções seguintes, o CEPD abordará três cenários abrangidos pela pergunta 4 do pedido, em que as diferenças residem em saber se os dados pessoais tratados para desenvolver o modelo são conservados no modelo e/ou se o tratamento subsequente é realizado pelo mesmo ou por outro responsável pelo tratamento.

3.4.1 Cenário 1 Um responsável pelo tratamento trata ilegalmente dados pessoais para desenvolver o modelo, os dados pessoais são conservados no modelo e são posteriormente tratados pelo mesmo responsável pelo tratamento (por exemplo, no contexto da implantação do modelo)

119. Este cenário diz respeito à questão 4, alínea i), do pedido, na situação em que um responsável pelo tratamento trata ilegalmente dados pessoais (ou seja, por incumprimento do artigo 5.º, n.º 1, alínea a), do RGPD e do artigo 6.º do RGPD) para desenvolver um modelo de IA, o modelo de IA conserva informações relativas a uma pessoa singular identificada ou identificável e, por conseguinte, não é anónima. Os dados pessoais são posteriormente tratados pelo mesmo responsável pelo tratamento (por exemplo, no contexto da implantação do modelo). Relativamente a este cenário, o CEPD apresenta as seguintes considerações.

120. O poder da AC para impor medidas corretivas ao tratamento inicial (tal como explicado nos pontos 113, 114 e 115 supra) teria, em princípio, um impacto no tratamento subsequente (por exemplo, se a AC ordenar ao responsável pelo tratamento que eliminasse os dados pessoais que foram tratados ilegalmente, tais medidas corretivas não permitiriam a este último tratar posteriormente os dados pessoais que estavam sujeitos às medidas).

121. No que diz respeito especificamente ao impacto do tratamento ilegal na fase de desenvolvimento sobre o tratamento subsequente (por exemplo, na fase de implantação), o CEPD recorda que cabe às AC efetuar uma análise caso a caso que tenha em conta as circunstâncias específicas de cada caso.

122. **A questão de saber se as fases de desenvolvimento e de implantação envolvem finalidades separadas (que constituem, por conseguinte, atividades de tratamento separadas) e em que medida a falta de base jurídica para a atividade de tratamento inicial afeta a licitude do tratamento subsequente, deve ser avaliada caso a caso, em função do contexto do caso.**

[88] A este respeito, o Parecer 39/2021 do CEPD sobre se o artigo 58.º, n.º 2, alínea g), do RGPD pode servir de base jurídica para uma autoridade de controlo ordenar *ex officio* o apagamento de dados pessoais numa situação em que esse pedido não tenha sido apresentado pelo titular dos dados, n.º 28. Ver também, a este respeito, TJUE, acórdão de 14 de março de 2024, Processo C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), parágrafo 42.

123. Por exemplo, no que diz especificamente respeito à base jurídica do artigo 6.º, n.º 1, alínea f), do RGPD, quando o tratamento subsequente se baseia em interesses legítimos, o facto de o tratamento inicial ter sido ilícito deve ser tido em conta na avaliação do interesse legítimo (por exemplo, no que diz respeito aos riscos para os titulares dos dados ou ao facto de os titulares dos dados poderem não esperar esse tratamento subsequente). Nestes casos, a ilegalidade do tratamento na fase de desenvolvimento pode afetar a licitude do tratamento subsequente.

3.4.2 Cenário 2: Um responsável pelo tratamento trata ilegalmente dados pessoais para desenvolver o modelo, os dados pessoais são conservados no modelo e são tratados por outro responsável pelo tratamento no contexto da implantação do modelo.

124. Este cenário está relacionado com a pergunta 4, alínea i), do pedido. Difere do cenário 1 (na secção 3.4.1 do presente parecer), uma vez que os dados pessoais são posteriormente tratados por outro responsável pelo tratamento no contexto da implantação do modelo de IA.

125. O CEPD recorda que determinar as funções atribuídas a estes diferentes intervenientes no âmbito do quadro de proteção de dados é um passo essencial para identificar as obrigações aplicáveis ao abrigo do RGPD e quem é responsável por essas obrigações, e que as situações de responsabilidade conjunta pelo tratamento também devem ser tidas em conta na avaliação das responsabilidades de cada uma das partes ao abrigo do RGPD. Por conseguinte, as observações que se seguem devem ser consideradas elementos gerais que devem ser tidos em conta pelas autoridades de controlo, sempre que pertinente. Relativamente a este cenário 2, o CEPD apresenta as seguintes considerações.

126. Em primeiro lugar, importa recordar que, nos termos do artigo 5.º, n.º 1, alínea a), do RGPD, lido à luz do artigo 5.º, n.º 2, do RGPD, cada responsável pelo tratamento deve assegurar a licitude do tratamento que realiza e ser capaz de o demonstrar. Por conseguinte, as AC devem avaliar a licitude do tratamento realizado i) pelo responsável pelo tratamento que inicialmente desenvolveu o modelo de IA; e ii) pelo responsável pelo tratamento que adquiriu o modelo de IA e trata os dados pessoais por si próprio.

127. Em segundo lugar, as considerações feitas nos pontos 113, 114 e 115 são pertinentes no caso vertente, no que se refere ao poder de intervenção das AC relativamente ao tratamento inicial. O artigo 17.º, n.º 1, alínea d), do RGPD (apagamento de dados tratados ilicitamente) e o artigo 19.º do RGPD (obrigação de notificação relativa à retificação ou ao apagamento de dados pessoais ou à limitação do tratamento) podem, dependendo das circunstâncias do caso, também ser pertinentes neste contexto, por exemplo no que diz respeito à notificação que o responsável pelo tratamento que desenvolve o modelo deve efetuar em relação ao responsável pelo tratamento que utiliza o modelo.

128. Em terceiro lugar, em relação ao possível impacto da ilicitude do tratamento inicial no tratamento subsequente realizado por outro responsável pelo tratamento, essa avaliação deve ser realizada pelas autoridades de controlo caso a caso.

129. **As AC devem ter em conta se o responsável pelo tratamento que implementa o modelo efetuou uma avaliação adequada, como parte das suas obrigações de responsabilidade[89] para demonstrar a conformidade com o artigo 5.º, n.º 1, alínea a), e o artigo 6.º do RGPD, para verificar se o modelo de IA não foi desenvolvido através do tratamento ilegal de dados pessoais.** Essa avaliação pelas autoridades de controlo deve ter em conta se o responsável pelo tratamento avaliou alguns critérios não exaustivos, como a fonte dos dados e se o modelo de IA é o resultado de uma infração do RGPD, em especial se foi determinado por uma autoridade de controlo ou por um tribunal, de modo que o

[89] Artigo 5.º, n.º 2, e artigo 24.º do RGPD.

responsável pelo tratamento que implementa o modelo não possa ignorar que o tratamento inicial foi ilícito.

130. O responsável pelo tratamento deve considerar, por exemplo, se os dados provêm de uma violação de dados pessoais ou se o tratamento foi objeto de uma constatação de infração por parte de uma AC ou de um tribunal. **O grau de avaliação do responsável pelo tratamento e o nível de pormenor esperado pelas AC podem variar em função de diversos fatores, incluindo o tipo e o grau de riscos suscitados pelo tratamento no modelo de IA durante a sua implantação em relação aos titulares de dados cujos dados foram utilizados para desenvolver o modelo.**

131. O CEPD observa que o Regulamento Inteligência Artificial exige que os fornecedores de sistemas de IA de alto risco elaborem uma declaração de conformidade da UE[90] e que essa declaração contém uma declaração de que o sistema de IA pertinente cumpre a legislação da UE em matéria de proteção de dados[91]. O CEPD observa que essa autodeclaração não pode constituir uma constatação conclusiva de conformidade ao abrigo do RGPD. Pode, no entanto, ser tida em conta pelas AC ao investigarem um modelo de IA específico.

132. As mesmas considerações feitas nos termos do n.º 123 acima também são relevantes neste caso. Quando as AC verificarem se e como o responsável pelo tratamento avaliou a adequação do interesse legítimo como base jurídica para o tratamento que efetua, a ilegalidade do tratamento inicial deve ser tida em conta como parte da avaliação do interesse legítimo, por exemplo, avaliando os riscos potenciais que podem surgir para as pessoas cujos dados pessoais foram tratados ilegalmente para desenvolver o modelo. Diferentes aspetos, quer de natureza técnica (por exemplo, a existência de filtros ou de limitações de acesso colocadas durante o desenvolvimento do modelo, que o responsável subsequente pelo tratamento não pode contornar ou influenciar, e que podem impedir o acesso ou a divulgação de dados pessoais), quer de natureza jurídica (por exemplo, a natureza e a gravidade da ilegalidade do tratamento inicial), devem ser devidamente considerados no âmbito do teste de equilíbrio.

3.4.3 Cenário 3 Um responsável pelo tratamento trata ilegalmente os dados pessoais para desenvolver o modelo e, em seguida, assegura que o modelo é anonimizado, antes de o mesmo ou outro responsável pelo tratamento iniciar outro tratamento de dados pessoais no contexto da implantação

133. Este cenário diz respeito à pergunta 4, alínea ii), do pedido e refere-se a um caso em que um responsável pelo tratamento trata ilegalmente dados pessoais para desenvolver o modelo de IA, mas fá-lo de uma forma que garante que os dados pessoais sejam anonimizados, antes de o mesmo ou outro responsável pelo tratamento iniciar outro tratamento de dados pessoais no contexto da implantação. Em primeiro lugar, o CEPD recorda que as autoridades de controlo são competentes e têm o poder de intervir no que diz respeito ao tratamento relacionado com a anonimização do modelo, bem como ao tratamento efetuado durante a fase de desenvolvimento. Assim, as AC podem, dependendo das circunstâncias específicas do caso, impor medidas corretivas a este tratamento inicial (tal como explicado nos pontos 113, 114 e 115 supra).

134. Se for possível demonstrar que o funcionamento subsequente do modelo de IA não implica o tratamento de dados pessoais, o CEPD considera que o RGPD não se aplicaria[92]. Assim, a ilegalidade do tratamento inicial não deve, por conseguinte, afetar o funcionamento posterior do modelo. No

[90] Artigo 16.º, alínea g), e artigo 47.º do Regulamento Inteligência Artificial.
[91] Anexo V, ponto 5, do Regulamento AI.
[92] Considerando 26 do RGPD.

entanto, o CEPD salienta que uma mera afirmação do anonimato do modelo não é suficiente para o isentar da aplicação do RGPD e observa que as AC devem avaliá-lo tendo em conta, caso a caso, as considerações fornecidas pelo CEPD para abordar a pergunta 1 do pedido.

135. **Quando os responsáveis pelo tratamento tratarem posteriormente os dados pessoais recolhidos durante a fase de implantação, depois de o modelo ter sido anonimizado, o RGPD aplicar-se-á em relação a essas atividades de tratamento. Nestes casos, no que diz respeito ao RGPD, a legalidade do tratamento efetuado na fase de implantação não deve ser afetada pela ilegalidade do tratamento inicial.**

4 Observações finais

136. A AC da Irlanda é a destinatária do presente parecer, que será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

Pelo Comité Europeu para a Proteção de Dados

O Presidente / A Presidente

Anu Talus